UNIVERSIDAD NACIONAL DE INGENIERIA
RECINTO UNIVERSITARIO "SIMÓN BOLÍVAR"
FACULTAD DE ELECTROTECNIA Y COMPUTACION

TRABAJO MONOGRÁFICO

Propuesta para la certificación TIER II del Centro de Datos de la Dirección General de Ingresos.

PARA OPTAR AL TÍTULO DE INGENIERO EN COMPUTACIÓN

ELABORADO POR:

Br. Josseline Jazmín Gómez Urbina
2013-61165

TUTOR:

MSc. Ing. Lizette Carolina Duarte Mora

Managua, Nicaragua

09/11/2018

Resumen del Trabajo

La disponibilidad y reguardo de la información es de vital importancia para el desarrollo de las organizaciones. Para llevar un control adecuado sobre la información de una compañía, una de las medidas a tomar, es la creación de un espacio físico especializado para el manejo de equipos informáticos. Dentro de este lugar, conocido como centro de datos, se llevan a cabo ciertas operaciones que permiten el monitoreo y la seguridad de la información de la compañía. Adicionalmente, se ejecutan y optimizan procesos críticos de la organización. De esta manera, se gestiona la continuidad de las actividades laborales, minimizando el riesgo de interrupciones y pérdida de información.

Un centro de datos debe de ser un entorno especializado que cuide la información, los equipos y propiedad intelectual más valiosa de la empresa. Además son los responsables de procesar todas las transacciones de toda la organización.

La Dirección General de Ingresos DGI, es una institución descentralizada con autonomía administrativa y financiera, cuyo objeto es aplicar y hacer cumplir las Leyes, actos y disposiciones que establecen o regulan ingresos a favor del Estado, que están bajo la jurisdicción de la Administración Tributaria, a tal efecto, anualmente recibe una partida presupuestaria, para ejecutar el cumplimiento de sus fines e impulsar una mayor eficiencia en la recaudación de todos los tributos.

Dicha institución cuenta con el centro nacional de datos fiscales, que tiene como objetivo resguardar la información más importante y relevante de la institución.

El presente trabajo monográfico, “Propuesta de certificación TIER ll para el centro nacional de datos fiscales de la dirección general de ingresos (DGI)”, tiene como propósito diseñar una propuesta para obtener la certificación TIER ll teniendo en cuenta factores como disponibilidad, escalabilidad, seguridad, manejabilidad y desempeño todo esto contemplando normas y estándares de seguridad y operatividad de centro de datos bajo las regulaciones de la Norma TIA-942.

En el cuerpo del documento se presentará el alcance y las directrices que se deben de seguir para solución del problema. Se organiza en: Dedicatoria, introducción Antecedentes, Justificación, Objetivos, Marco teórico y el desarrollo del trabajo que se divide en un breve diagnóstico del Nivel de Tier en el que se encuentra el centro de datos de la dirección general de ingresos y en diez fases que se distribuyen a nivel de infraestructura en los sistemas: eléctrico, climatización, seguridad física, comunicaciones. También se muestra un prototipo de un centro de Datos que cumple con los estándares de la norma TIA 942 para una certificación TIER ll.

Contenido

Lista de figura

Dedicatoria

A Dios por haberme dado la sabiduría para lograr terminar con éxito esta etapa.

A mi madre por su apoyo incondicional en este largo y arduo camino, por enseñarme que cuando se trabaja con esfuerzo, dedicación y humildad todo es posible.

A mis hermanas por estar en cada momento de mi vida, por animarme siempre a salir adelante a pesar de las dificultades.

A mi familia que siempre me apoyo durante toda mi carrera y estuvo acompañándome en todo momento. Gracias a ellos logré cumplir mis metas y salir adelante durante este camino.

A mi tutora *MSc. Ing. Lizette Carolina Duarte Mora* que me guio y me apoyo a lo largo de este trabajo, mostrando su compromiso e interés por que todo saliera adelante.

Josseline Jazmín Gómez Urbina

Introducción

En cualquier empresa los centros de datos llevan a cuestas la labor de almacenar y procesar toda la información que se genera al interior de la organización.

La mejor manera de mantener un buen funcionamiento del centro de datos es seguir las mejores prácticas de compañías líderes a nivel mundial y contar con certificaciones que avalen su correcta operación. Uno de los estándares más importantes es otorgado por el Uptime Institute, una organización que brinda asesoría para gestionar la infraestructura critica de la empresa.

De acuerdo a los datos de la firma, hasta a ahora han certificado a más de 1,000 Centro de datos alrededor del mundo, por su diseño, construcción, administración y operación. (Institute, 2018)

La certificación Tier es el resultado del trabajo de un grupo de expertos en data centers para establecer una serie de políticas de desempeño, con el objetivo de garantizar el correcto funcionamiento de este tipo de infraestructura. Esta clasificación es equiparable a los estándares ISO o CMMI y se enfoca únicamente a la evaluación de los centros de datos. De acuerdo con información del Uptime Institute, hay cuatro niveles que la operación de la infraestructura del centro de datos debe cumplir; éstos son incrementales, lo cual quiere decir que si un data center es clasificado como Tier II, debe ser primero Tier I para obtener el siguiente nivel.

Cada Tier toma en cuenta aspectos como la disponibilidad, la alimentación eléctrica, el enfriamiento, los componentes redundantes, entre otros.

En el presente documento se plasmará una propuesta para la certificación del centro de datos de la dirección general de ingresos (DGI) en nivel de Tier ll utilizando como referencia la norma TIA-942. Lo cual ayudara a tener una visión del funcionamiento e infraestructura del centro Nacional de Datos Fiscales.

Justificación

El desarrollo y evolución de los centros de datos, demandó inicialmente la necesidad de diseñar y construir el centro de datos con las mejores prácticas del mercado, buscando optimización, estandarización y facilitar el mantenimiento y la operación.

Cuando tenemos un producto o servicio es necesario evaluarlo para determinar su finalidad. Sus características tienen que ser normalizadas en un documento denominado “Norma”. Para ello debe haber un acuerdo de sus fabricantes, usuarios, autoridades u asociaciones profesionales, entre otros.

Sabiendo esto una certificación de calidad es el resultado de un proceso por el cual los auditores o evaluadores de la empresa certificadora examinan la conformidad de ese producto o servicio según los requisitos de la norma. Si el resultado es satisfactorio se emitirá pues un documento público: el certificado.

En el aspecto de comunicación externa la empresa que posee un certificado de calidad destaca en el mercado de su ámbito de servicios de aquellos que no lo tienen. Por tanto, asegura un incremento en la reputación e imagen de empresa.

En comunicación interna se desarrolla una mejora continua entre los trabajadores con una eficacia y eficiencia de los procesos como prácticas habituales en su gestión.

Actualmente el Centro Nacional de Datos Fiscales de la Dirección General de Ingresos (DGI) no cuenta con ninguna certificación. Lo que se pretende con esta propuesta es ver los beneficios de implementar una norma para la certificación en TIER nivel ll, así como también minimizar las vulnerabilidades e incidentes que puedan ocurrir y mostrar los beneficios de tener un centro de datos certificado siguiendo los estándares establecidos.

Objetivos

Objetivo General:

Elaborar una propuesta de certificación TIER ll que permita evaluar los niveles de cumplimiento de la norma TIA-942 en el Centro Nacional de Datos Fiscales de la Dirección General de Ingresos (DGI).

Objetivos específicos:

- ✓ Analizar la importancia y los beneficios de implementar la norma TIA-942 para la certificación TIER ll.
- ✓ Evaluar los niveles de cumplimiento del centro de datos de la dirección general de ingresos con respecto a la norma TIA-942.
- ✓ Presentar un prototipo de centro de centro de datos con certificación TIER ll
- ✓ Minimizar el impacto de la vulnerabilidad e incidentes en el Centro Nacional de Datos Fiscales (CNDF).
- ✓ Proponer los beneficios que se obtendrían con certificación del Centro Nacional de Datos Fiscales.

Marco teórico

El presente Marco Teórico define las bases conceptuales adecuadas al problema a resolver y sobre el cual se sustenta todo el trabajo a realizar en esta investigación, para ello se requiere reconocer los términos relacionados al área del desempeño en el cual se desarrollaran en el cuerpo de documento.

Definición Certificación TIER:

TIER es una certificación o “clasificación” de un centro de datos en cuanto a su diseño, estructura, desempeño, fiabilidad, inversión y retorno de inversión. Uptime Institute creó el sistema Tier Classification estándar para evaluar de manera efectiva la infraestructura de los centros de datos en términos de los requisitos de una empresa para la disponibilidad de sistemas. El sistema Tier Classification ofrece a la industria de los centros de datos un método coherente para comparar las instalaciones personalizadas y normalmente únicas en función del rendimiento o el tiempo de productividad esperado de la infraestructura del sitio. Además, los Tiers les permiten a las compañías alinear las inversiones en la estructura de su centro de datos con los objetivos comerciales específicamente relacionados con las estrategias tecnológicas y de crecimiento.

Esta certificación es otorgada por el Uptime Institute, una división independiente de la empresa The 451 Group con sede central en Nueva York. El Uptime Institute está conformado por destacados miembros de la industria de infraestructura de sistemas, consultores especializados y usuarios del servicio a nivel internacional. (Institute, 2018)

Figura 1. Uptime Institute Tier Certification Map.

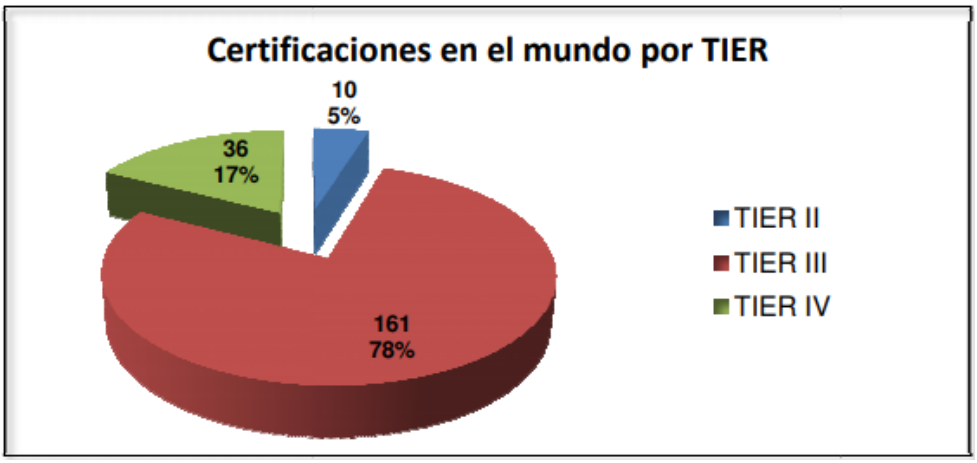


Figura 2. Certificaciones en el mundo TIER

Según los datos de la figura 2 la gran mayoría de las certificaciones a nivel mundial es la TIER lll con una participación del 78%, seguida de lejos por el TIER lV y por el TIER ll no hay certificaciones del TIER l.

Tipos de Certificaciones:

TIER I: Centro de datos Básico

Un centro de datos TIER l puede ser susceptible a interrupciones, tanto planeadas como no planeadas. Cuenta con sistema de aire acondicionado y distribución de energía, pero puede tener o no piso técnico, UPS o generador eléctrico; si los posee pueden no tener redundancia y existir varios puntos únicos de falla, la carga máxima de los sistemas en situaciones críticas es del 100%. (TIA-942, 2018)

La infraestructura del Centro de datos deberá estar fuera de servicios al menos una vez al año por razones de mantenimiento y/o reparaciones. Situaciones de urgencia pueden motivar paradas más frecuentes y errores de operación o fallas en los componentes de infraestructura causaran la detención del centro de datos.

La tasa de disponibilidad del centro de datos es de 99.671% del tiempo.

TIER II: Centro de datos Redundante

Componentes redundantes; los centros de datos con componentes redundantes son ligeramente menos susceptibles a interrupciones tanto planeadas como no planeadas, estos centro de datos cuentan con piso falso, UPS, generadores eléctricos pero están conectados a una sola línea de distribución eléctrica su diseño es lo necesario más uno (N+1) lo que significa que al menos hay un duplicado de cada componente de la infraestructura. La carga máxima de los sistemas d situaciones críticas es del 100%. El mantenimiento de la línea de la distribución eléctrica o en otros componentes de la infraestructura puede causar una interrupción del procesamiento. (TIA-942, 2018)

La tasa de disponibilidad del centro de datos es 99.749% del tiempo.

TIER III: Centro de datos Concurrentemente Mantenibles

Las capacidades de un centro de datos de este tipo le permiten realizar cualquier actividad planeada sobre cualquier componente de la infraestructura sin interrupciones en la operación. Actividades planeadas permiten mantenimiento preventivo y programado, reparaciones o reemplazo de componentes, agregar o eliminar elementos y realizar pruebas de componentes o sistemas, entre otros. Para infraestructura que utilizan sistemas de enfriamiento por agua significa doble conjunto de tuberías.

Debe de existir suficiente capacidad y doble línea de distribución, de los componentes de forma tal que sea posible realizar los mantenimientos o pruebas en una línea, mientras que la otra atiende la totalidad de la carga. En este TIER, actividades no planeadas como errores de operación o fallas espontaneas en la infraestructura, pueden todavía causar una interrupción del centro de datos. La carga máxima de los sistemas en situaciones críticas es de 90%.

Muchos Centros de datos TIER lll son diseñados para poder actualizarse en TIER lV, cuando los requerimientos del negocio justifiquen el costo. (TIA-942, 2018)

La tasa de disponibilidad máxima del centro de datos es 99.982% del tiempo.

TIER IV: Centro de datos Tolerante a fallos

Este centro de datos provee capacidad para realizar cualquier actividad planeada si interrupciones en las cargas críticas, pero además la funcionalidad tolerante a fallas le permite a las infraestructuras continuar operando aun ante un evento crítico no planeado. Este requiere dos líneas de distribución simultáneamente activas, típicamente en una configuración system + system, eléctricamente esto significa dos sistemas de UPS independientes, cada sistema con un nivel de redundancia (N+1) la carga máxima de los sistemas en situaciones críticas es del 90% y persiste un nivel de exposición a fallas, por el inicio una alarma de incendio o porque una persona inicie un procedimiento de apagado de emergencia o Emergency Power

Off (EPO), los cuales deben existir para cumplir con los códigos de seguridad contra incendios. (TIA-942, 2018)

La tasa de disponibilidad máxima del centro de datos es 99.995% del tiempo.

Norma TIA-942

La ***Telecomunication Industry Association*** publica su estándar TIA-942 con la intención de unificar criterios en el diseño de áreas de tecnología y comunicaciones. Este estándar que en sus orígenes se basa en una serie de especificaciones para comunicaciones y cableado estructurado, avanza sobre los subsistemas de infraestructura generando los lineamientos que se deben seguir para clasificar estos subsistemas en función de los distintos grados de disponibilidad que se pretende alcanzar. En su anexo G (informativo) y basado en recomendaciones del Uptime Institute, establece cuatro niveles (Tiers) en función de la redundancia necesaria para alcanzar niveles de disponibilidad de hasta el 99.995%.

El estándar TIA 942 y la categorización de Tiers en Latinoamérica llevan al replanteamiento de las necesidades de infraestructura para la instalación de un centro de datos. (García Enrich , 2018)

Según el estándar TIA-942, la infraestructura de soporte, la infraestructura de soporte de un centro de datos debe estar compuesto por cuatro subsistemas como lo son telecomunicaciones, arquitectura, sistema eléctrico y sistema mecánico. (TIA-942, 2018)

El estándar TIA 942 y la categorización de TIER se encuentran en pleno auge en américa latina. Esto es bueno porque leva el replanteo de las necesidades de infraestructura de una manera racional y alineada con las necesidades propias de disponibilidad del negocio en que se encuentra las organizaciones. (TIA-942, 2018)

Norma ANSI/BICSI 002

Se considera la norma base para el diseño de base de datos alrededor del mundo, ANSI/BICSI 002 continúa su misión de proporcionar requisitos, directrices y mejores prácticas, aplicables al centro de datos.

BICSI 002 integra los conceptos clave y las necesidades de otros documentos y normas como ISO, IEC, TIA, ASHRAE, NFPA y otros, al tiempo que proporciona referencias específicas y consideraciones para el manejo de información. Esta función única de BICSI 002, proporciona un documento completo, que es aplicable en todo el mundo. (BICSI, 2018)

La dirección general de ingresos cuenta con el centro nacional de datos fiscales que cuenta con sistemas redundantes que lo hace menos susceptible a interrupciones planeadas y no planeadas, la dirección general de ingresos cuenta con una infraestructura de centro de datos que puede estar fuera de servicio una vez al año por razones de mantenimiento o reparaciones. (DGI, 2018)

Diseño Metodológico

Se hará uso de la **Norma TIA-942** como metodología para determinar las fases necesarias para el análisis y evaluación del Centro de Datos y así poder determinar los niveles de cumplimiento de la norma para la certificación **TIER II** ya que la norma provee directrices para el diseño y e instalación de un centro de datos la cual será utilizado para definir la necesidades de infraestructura de un centro de datos **TIER II** basado en una serie de especificaciones que genere lineamientos que se debe de seguir para clasificar el centro de datos en función de los distintos grados de disponibilidad que se pretenden alcanzar. Se elaboró un breve diagnóstico del grado de certificación del centro de datos de la dirección general de ingresos y un prototipo con las especificaciones establecidas por la norma TIA-942 en nivel de certificación TIER ll.

Se desarrollaron las siguientes etapas:

Fase I: Evaluación del Sitio.

En esta etapa se describe los lineamientos que debe seguir para la evaluación del ubicación ideal del sitio para que ofrezca calidad que un centro de datos por sí mismo ofrece a una empresa, en esta fase se determina qué tan apropiada es la zona donde se ubica. Buscar y determinar los factores de riesgo del lugar ya que cada pedazo de terreno tiene sus propias fallas. Conocer el sitio ideal es muy útil y debe ser tomado en cuenta muy seriamente.

Fase II: Evaluación del Espacio.

En esta etapa se evalúa el espacio que debe de tener un centro de datos con nivel Tier ll para la colocación de equipos en el espacio físico del mismo.

Fase III: Evaluación Arquitectónico.

En esta etapa se desarrolló un paso crucial a la hora de reducir los riesgos vinculados a un centro de datos, muchos de los centros de datos se han construido

Con los más elevados niveles de disponibilidad, pero en lugares equivocados. Se desarrolló los pasos necesarios para la evaluación arquitectónica de un centro de datos con nivel TIER ll.

Fase IV: Evaluación del Sistema Eléctrico.

En esta fase se toma en cuenta las recomendaciones que tiene que tener los equipos en el centro de datos que está sujetos a frecuentes cambios de corriente, cortes y variaciones de corriente, los equipos experimentarán fallas que no sucederían si trabajarán con fuentes de energía estables. Para garantizar esto se debe tener en cuenta la alimentación de las distintas fuentes de energía que se encuentren disponibles de manera independiente o a través de mallas de energía.

Fase V: Evaluación del Sistema Mecánico.

En esta fase se desarrolló el sistema mecánico que se utiliza en un centro de datos con certificación Tier ll.

Fase VI: Evaluación de la Protección contra incendios.

En esta etapa se desarrollara los requisitos importantes para la protección del equipamiento de tecnología de la información y de las áreas para los equipos de tecnología de la información, de los daños ocasionados por el fuego o por sus efectos asociados, es decir, humo, corrosión, calor y agua.

Fase VII: Evaluación de la Seguridad.

En la siguiente etapa se consideró aspectos importantes como la seguridad en el acceso a las instalaciones para evitar fugas de información o daños bajo las regulaciones TIA-942.

Fase VIII: Evaluación de la Infraestructura, vías y espacios de cableado de telecomunicaciones.

En esta etapa se determinó las opciones en cables, cuántas conexiones se proveerán, y como estarán organizadas las terminaciones. También se tomó en cuenta la conexión directa de los servidores a los gabinetes.

Fase IX: Evaluación de las TI.

En esta fase se midió el desempeño de las TI proporciona elementos clave para decidir sobre el gasto que se hará, la continuidad de proyectos y la necesidad de inversión en nuevas tecnologías que permitan generar valor.

Fase X: Evaluación de la infraestructura usando Tiers.

En esta etapa se elaboró tablas con el listado de regulaciones establecidos por la norma TIA-942 y los niveles de TIER otorgados por la Uptime Institute se evalúan el nivel de cumplimiento de un centro de datos con certificación TIER ll.

Diagnostico

Se hizo una encuesta al área de unidad de bases de datos y sistemas operativos que está a cargo del centro del datos de la Dirección general de ingreso tomando en cuenta las especificaciones de la norma TIA- 942 para hacer un breve diagnóstico del nivel de certificación de TIER del centro nacional de datos fiscales de la dirección general de ingresos. Utilizando SPSS para generar las estadísticas arrojadas con la con la encuesta realizada al personal de informática.

En la encuesta realizada se tocó los puntos claves con los que debe de contar el centro de datos con Certification TIER ll generando así el resultado con un nivel de cumplimiento el 98 % de los encuestados concluye que cumple con los puntos clave de nivel TIER ll.

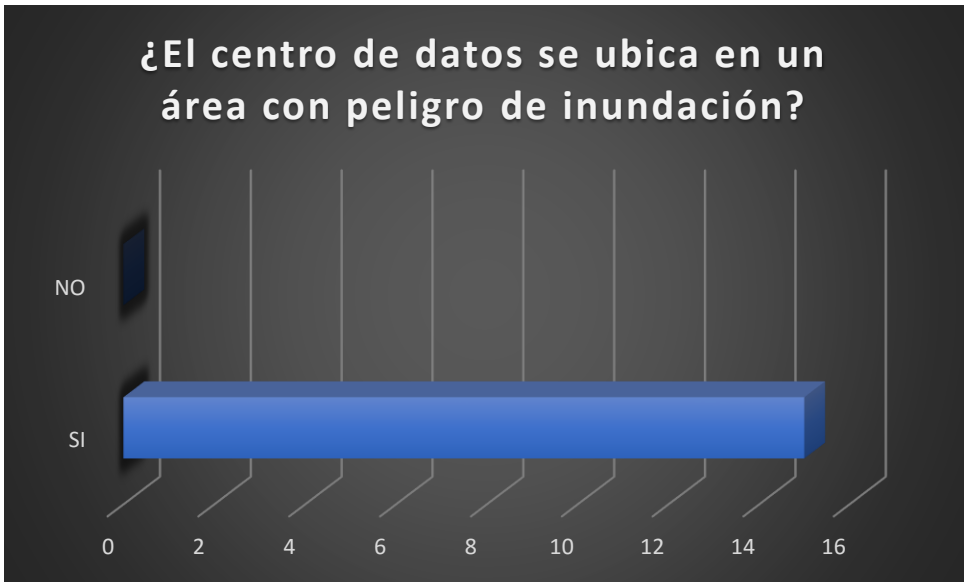


Figura 3: Respuesta # 01 de la encuesta

En el siguiente diagrama el personal de informática coincide que el centro de datos no se encuentra en un área de riesgo de inundación.

Figura 4: Respuesta # 02 de la encuesta

El siguiente grafico muestra los resultados de 13 personas que afirman que los gabinetes y rack se encuentran rotulados 2 personas afirman que no lo están.

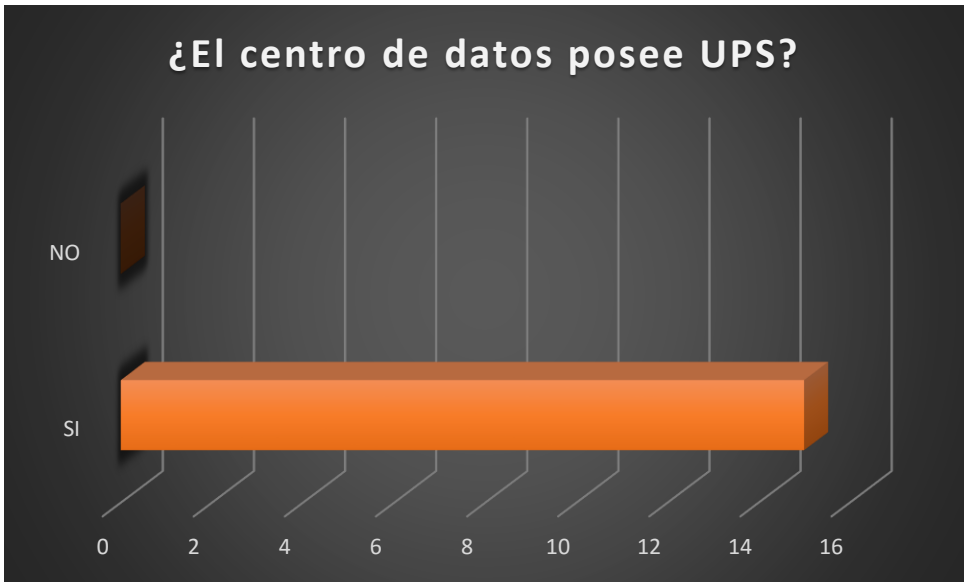


Figura 5: Respuesta # 03 de la encuesta

En siguiente grafico muestra que las 15 personas encuestadas afirman que el centro de datos posee ups.

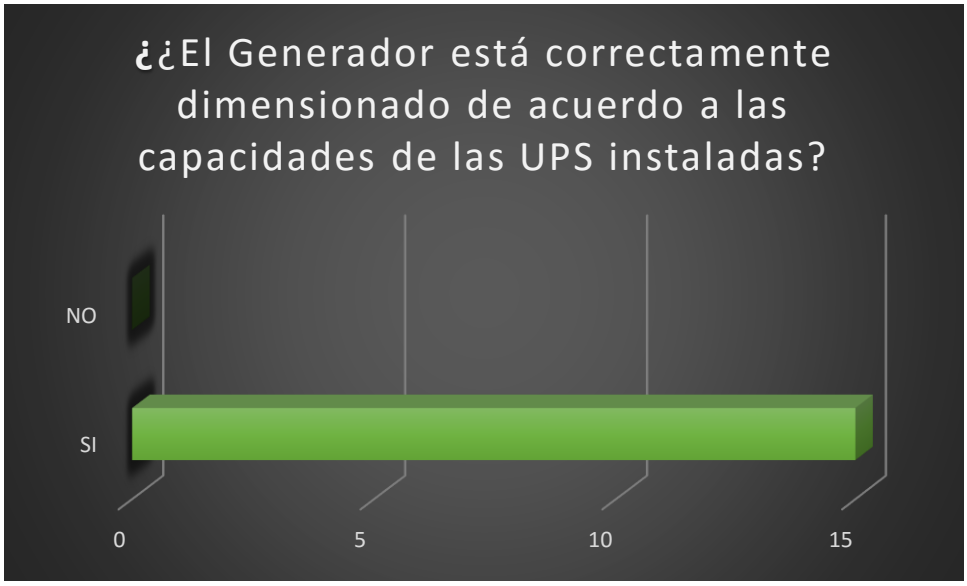


Figura 6: Respuesta # 04 de la encuesta

El siguiente grafico de barra muestra que las 15 personas encuestadas afirman que el generador del centro de datos está correctamente dimensionado para las ups instaladas.

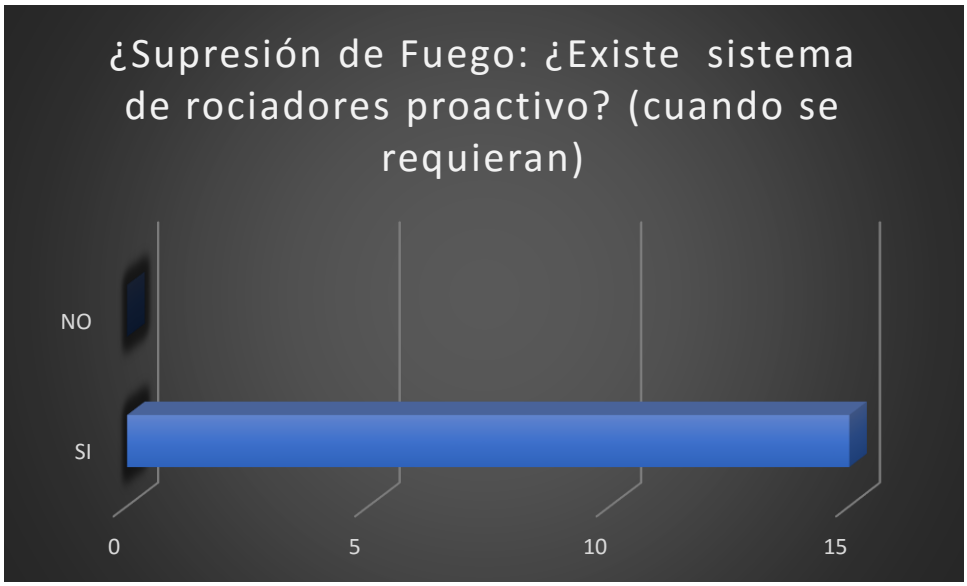


Figura 7: Respuesta # 05 de la encuesta

El siguiente grafico de barra muestra que las 15 persona encuestadas afirman existe supresión de fuego en el centro de datos.

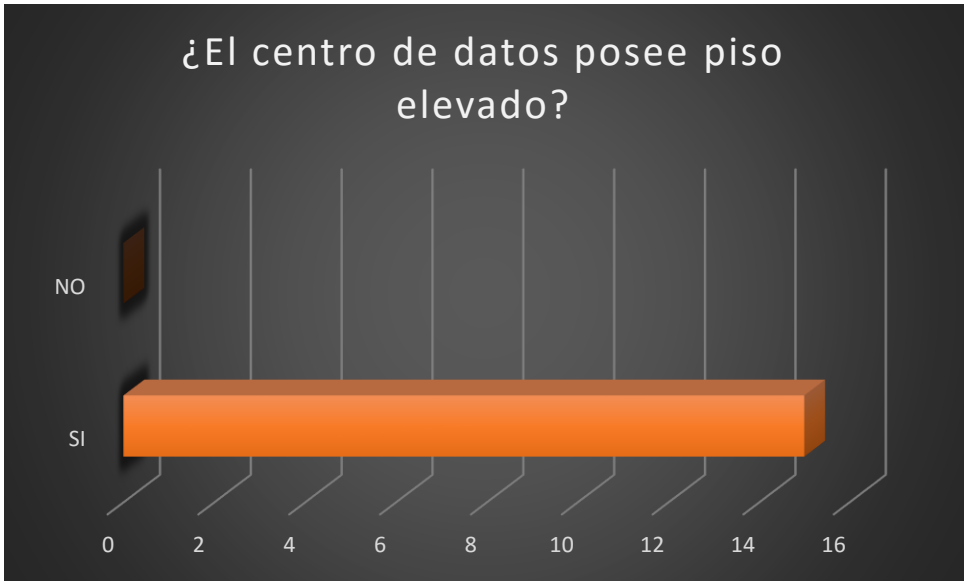


Figura 8: Respuesta # 06 de la encuesta

El siguiente grafico de barra muestra que las 15 persona encuestadas afirman que el centro de datos posee piso elevado.

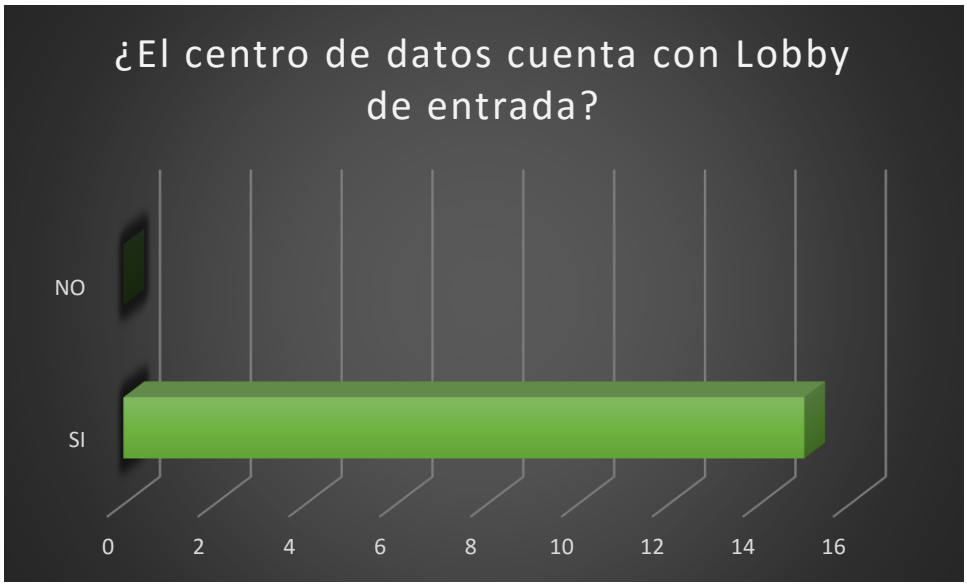


Figura 9: Respuesta # 07 de la encuesta

El siguiente grafico de barra muestra que las 15 persona encuestadas afirman que el centro de datos posee lobby de entrada.

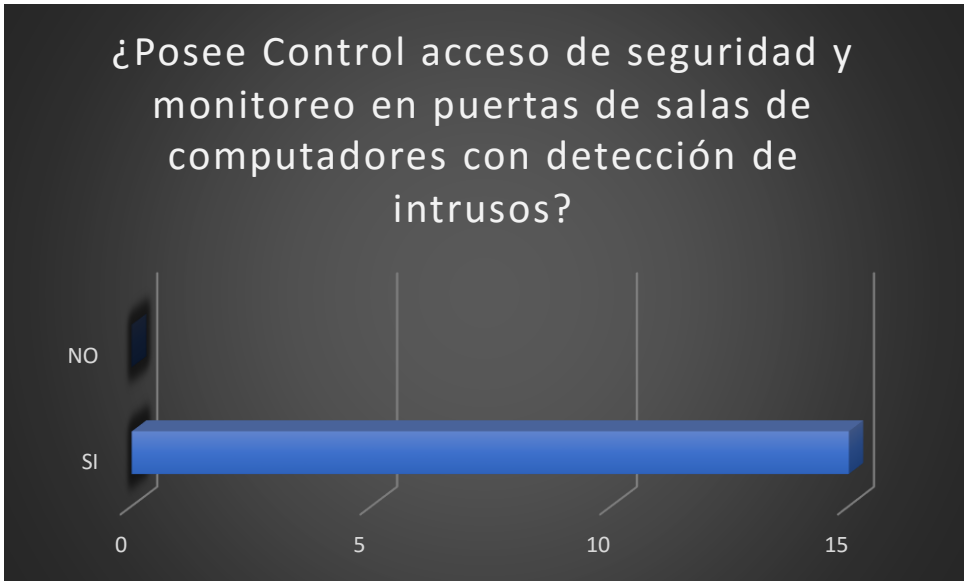


Figura 10: Respuesta # 08 de la encuesta

El siguiente grafico de barra muestra que las 15 persona encuestadas afirman que el centro de datos posee control de acceso en la salas de computadores.

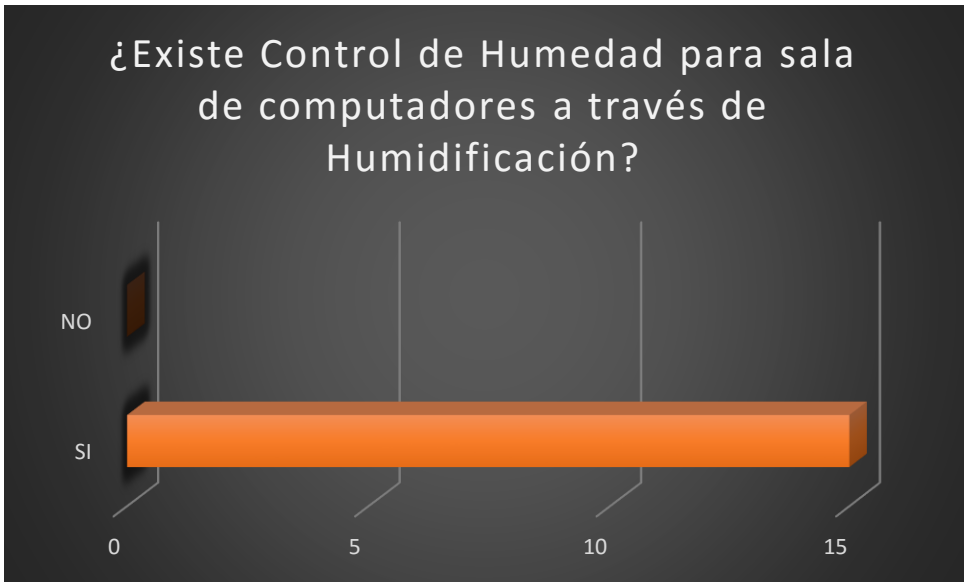


Figura 11: Respuesta # 09 de la encuesta

El siguiente grafico de barra muestra que las 15 persona encuestadas afirman existe control de humedad para las salas de computadoras

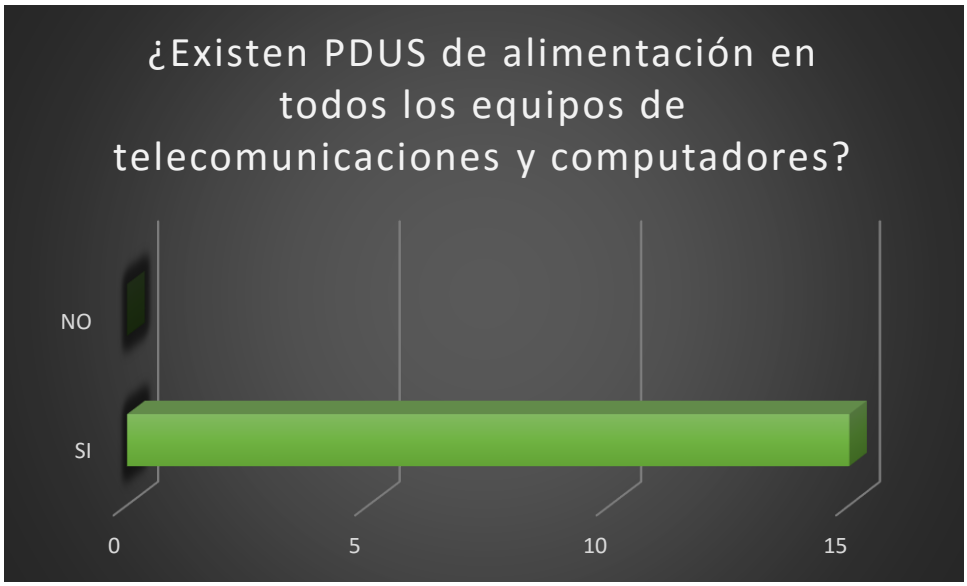


Figura 12: Respuesta # 10 de la encuesta

El siguiente grafico de barra muestra que las 15 personas encuestadas afirman existe PDU para los equipos de telecomunicaciones.

Fase I: Evaluación del Sitio.

1.1 Introducción.

Dentro del centro de datos hay servidores para los servicios ofrecidos en la institución contiene los datos de millones de usuarios por lo cual es importante es evaluar el lugar del sitio donde se encuentran alojados los servidores en los siguientes incisos se aborda las recomendaciones para la evaluación adecuada del sitio.

1.2 Evaluación del Sitio

1.2.1Instalaciones Cercanas al sitio.

Las siguientes instalaciones deberían situarse a un mínimo de 13 kilómetros de distancia:

• Aeropuertos menores
• Bases o instalaciones de control de misiles
• Bases militares
• Otras instalaciones militares.

Las siguientes instalaciones deberían situarse a un mínimo de 8 kilómetros de distancia:

• Aeropuertos importantes
• Planta de productos químicos y fertilizantes
• Sitios de almacenamiento de cereales
• Depósitos de gas, gasolina, combustible, petróleo
• Otras industrias pesadas

Las siguientes instalaciones deberían situarse a un mínimo de 5 kilómetros de distancia:

• Embajadas
• Grupos políticos extremos
• Laboratorios de investigación
• Instalaciones meteorológicas y de radar de otro tipo
• Transmisores / cadenas de radio/ televisión

Las siguientes instalaciones deberían situarse a un mínimo de 3.2 kilómetros de distancia:

• Vertederos
• Basureros
• Chatarrerías
• Canteras
• Autopistas importantes
• Instalaciones ferroviarias
• Puertos / Canales internos
• Plantas de tratamiento de aguas residuales y municipales
• Áreas de explotación ganadera
• Granjas de cebado, criaderos
• Lagos
• Presas
• Embalses

Las siguientes instalaciones deberían situarse a un mínimo de 1.6 kilómetros de distancia:

• Estaciones de gas
• Distribuidores de gas comprimido
• Repuestos automotores u otros talleres de pintura
• Instalaciones de auto-almacenamiento
• Líneas de distribución de energía de alta tensión
• Subestaciones de servicios públicos
• Torres de almacenamiento de agua Importancia de la disponibilidad de recursos en la elección del sitio

• Servicios básicos de energía: Calidad del suministro eléctrico, distintas rutas, separación de rutas, ampliación de capacidad, fuentes de alimentación, costo energético.

• Gas: Suministro mediante tuberías, distintas rutas, depósitos de almacenamiento, varios proveedores. (BICSI, 2018)

• Agua: Disponibilidad, suministro directo mediante tuberías, suministro natural adyacente, por ejemplo, ríos, lagos, etc., capacidad de expansión.

• Telecomunicaciones: Varios proveedores, Distintas rutas, capacidad existente y de expansión.

• Calidad del aire: Niveles de humedad, partículas transportadas en el aire, contaminación del aire, lluvia acida. (BICSI, 2018)

1.3 Identificar los Peligros Naturales

Un Data Center está expuesto a riesgos que pueden ser referentes a la infraestructura o causados por amenazas físicas.
(TI, 2018)

Los riegos fiscos abarcan desde incendio de grandes proporciones hasta un simple vaciamiento de agua en el centro de datos. Calor, Humo y gases corrosivos deben ser evitados, pues dañan hardware y datos.
(TI, 2018)

1.4 Algunos de los peligros naturales identificados:

Actividad sísmica: La actividad sísmica (terremotos) comúnmente se relaciona con la presencia de un volcán o falla geológica. Los terremotos pueden fluctuar desde un movimiento con un nivel mínimo de vibración que dure menos de un segundo a un evento catastrófico con una duración mayor a 20 segundos, que ocasionara grandes daños o destrucción en la estructura del área del suceso.

En lo posible deberían evitarse las áreas de actividad sísmica, si ello no es posible, se deberán emplear estructuras y apoyo de equipos sísmicos adecuados para cumplir o exceder los requisitos impuestos.

En un área de actividad sísmica el equipo dentro del centro de datos incluyendo gabinetes y bastidores de equipo de la tecnología de la información, debería de diseñarse según el nivel de actividad sísmica que puede soportar el centro de datos e incluir el anclaje estructural correspondiente. Además los requisitos estructurales del edificio serán más rigurosos (BICSI, 2018)

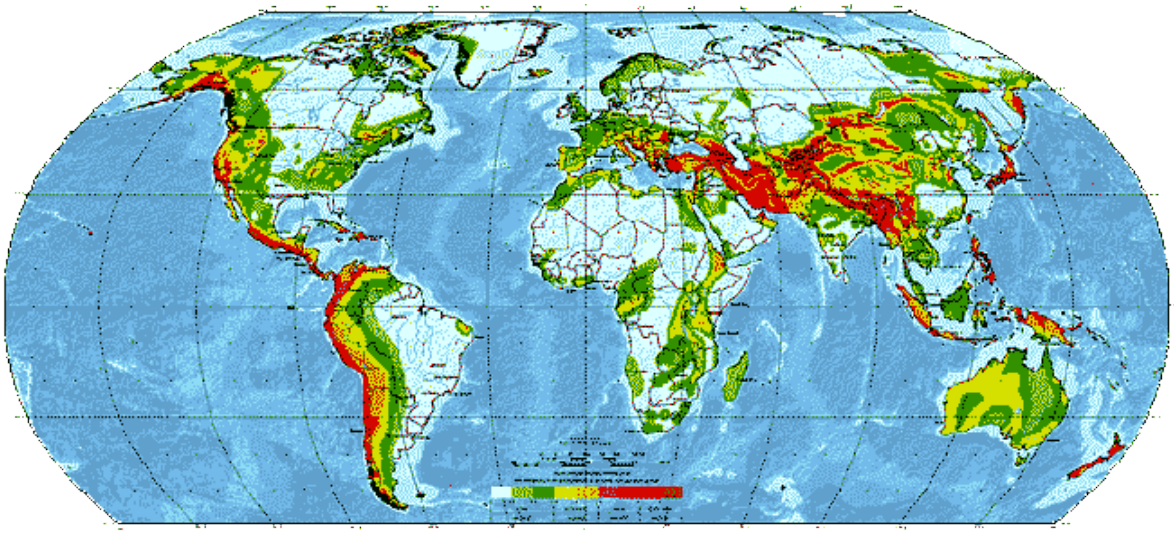


Figura 13. Mapa de peligro sísmico a nivel mundial

Actividad volcánica: Los volcanes deben de encontrase cerca de las fallas geológicas, por otra parte los volcanes representan un riego adicional derivado de una erupción y subsiguiente flujo de lava, ceniza volcánica, lahares o inundación.

Los centros de datos deben situarse fuera de área del riesgo inmediata (En una zona de seguridad) respecto a un volcán activo, es preciso obtener información sobre las zonas peligrosas de todo volcán.

Fuego incontrolado: Los incendios pueden propagarse fácilmente en 6,000 hectáreas (15,000 acres) o en un área mayor. Aunque probablemente un sitio no esté expuesto a un riesgo inmediato, los incendios que ocurren a 80 km (50 millas) o a una mayor distancia pueden afectar la infraestructura de transmisiones del proveedor de acceso utilizada por el centro de datos.

Los fuegos incontrolados comúnmente ocurren lejos de entornos urbanos. Sin embargo, dependiendo de la topografía del área y de la cantidad de otras urbanizaciones en la zona, algunos sitios están propensos a una interrupción operativa o a daños estructurales debido a incendios.

Los centros de datos no debieran emplazarse en el límite de una zona de desarrollo urbano ni cerca de áreas naturales protegidas. Los sitios para centros de datos en áreas que sean conocidas por acontecimientos de fuegos incontrolados debieran consultar todos los antecedentes del proveedor de acceso en cuanto a las interrupciones del servicio debido a incendios.

Si se desea colocar un centro de datos dentro de un área con riesgo de incendio moderado a alto, debiera contemplarse el uso de rutas de ingreso redundantes para conferir acceso al sitio tanto a los operadores del centro de datos como a las cuadrillas de supresión de incendios. Los planes de seguridad y recuperación ante desastres deben incluir procedimientos detallados sobre evacuaciones y operaciones continuadas del centro de datos en caso de que sea necesario desalojar un sitio debido a un incendio. (BICSI, 2018)

Terrenos inundables: Las inundaciones pueden ocurrir en numerosas áreas y en zonas en las que no suele haber flujo significativo de lluvias o nevadas al año.

Se recomienda seleccionar un sitio que no presente riesgos de inundaciones derivadas de llanuras aluviales de ríos en las proximidades, cuencas tidales en las proximidades, fallas de represas, tsunamis o fallas de diques. El sitio no debiera estar dentro de zonas de inundación por tsunamis y peligros de aluviones según se

define en IBC 2012, estar dentro de 91 m (300 pies) respecto a un área de peligro de inundación por 500 años, o estar a menos de 3 m (10 pies) por sobre el máximo nivel de inundación conocido. El sitio también debiera contar con múltiples accesos a carreteras cuya altura se encuentre sobre los niveles de inundación recomendados a lo largo de toda la ruta.

1.5 Identificar los Peligros Generados por Personas

Existen algunos peligros generados por personas entre los cuales podrían estar desorden civil, terrorismo, vandalismo, acceso no autorizado al centro de datos.

Se debe Asegurar de que los sistemas de seguridad del edificio están operativos.

1.6 Ubicación y acceso al sitio

Dentro de las principales prevenciones está el acceso limitado, evitando así una acción inadecuada dentro del centro de datos. Para esto se debe de contar con un control de acceso relacionados con métodos de identificación.

Los métodos adecuados son por la identificación de la identidad de la persona, esto implica un reconocimiento físico; este método es llamado biometría. Algunas de las características físicas que se utilizan son: Las huellas, el iris, la retina o la voz. (TIA-942, 2018)

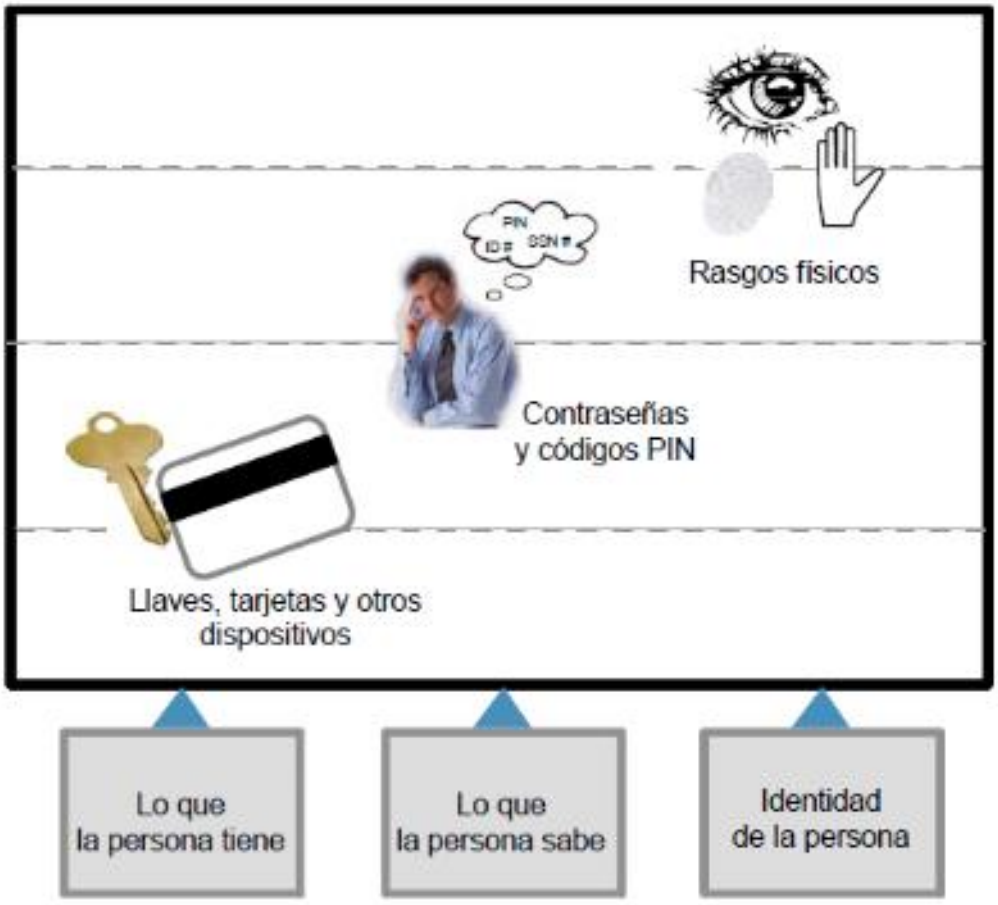


Figura 14. Niveles de seguridad en un centro de datos

1.7 Servicios Públicos

Servicio eléctrico y energético:

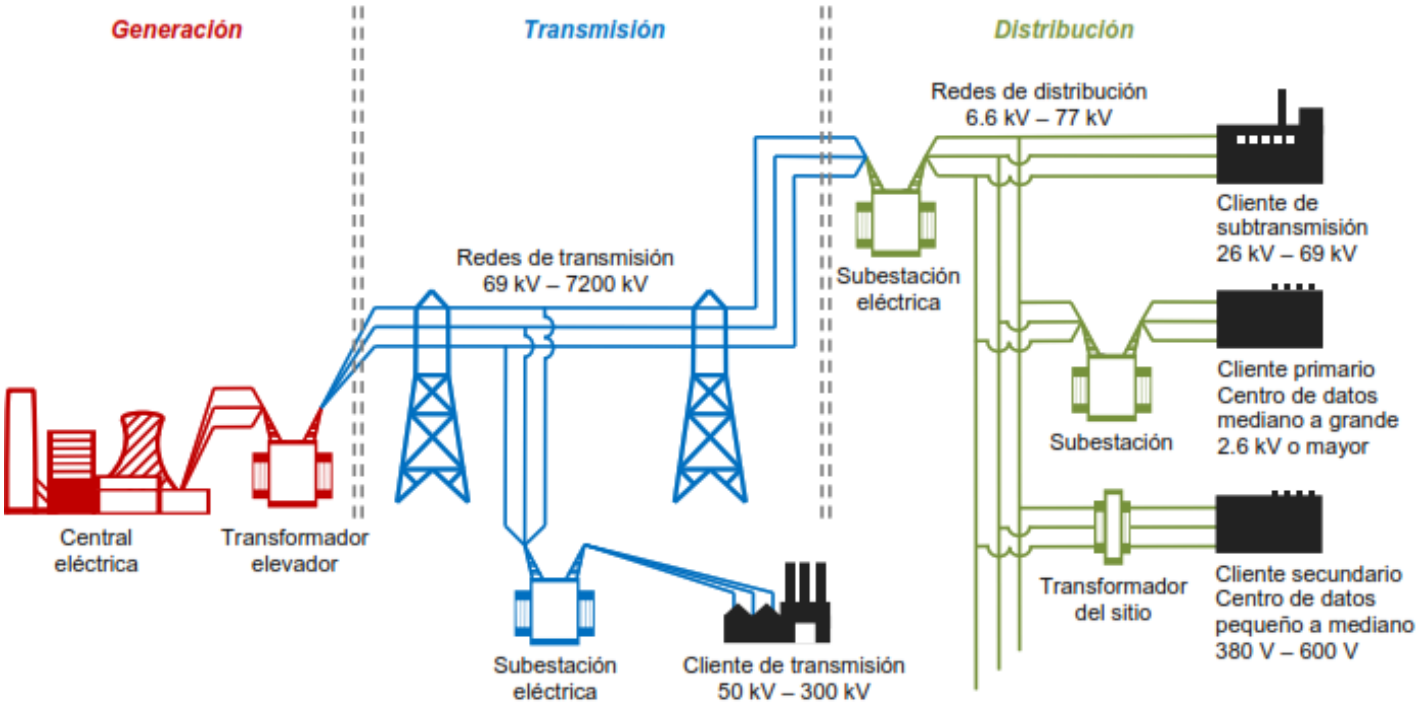


Figura 15. Estación eléctrica de centrales eléctricas a centro de datos

Los alimentadores de entrada del servicio eléctrico deberían de tener 1.2m (4 pies) respecto a otros servicios públicos a lo largo de todo el trayecto. Si se proporcionan alimentadores redundantes en el centro de datos, se recomienda que las entradas de servicio eléctrico de la instalación tenga una separación mínima de 20 m (66 pies) respecto a las demás entradas de servicio eléctrico a lo largo de todo el trayecto.

(TIA-942, 2018)

A continuación se incluye una lista con las fuentes preferidas de electricidad (En Orden correlativo.

1) Al menos dos alimentadores de servicio eléctrico tendidos divergentemente.
2) Diferentes subestaciones ubicadas en redes eléctricas independientes.
3) Al menos dos alimentadores de servicio eléctrico tendidos divergentemente. desde diferentes subestaciones ubicadas en la misma red eléctrica.
4) Al menos dos alimentadores de servicio eléctrico tendidos divergentemente
5) desde una sola subestación.
6) Un alimentador de servicio eléctrico desde una sola subestación.

- Servicio eléctrico subterráneo.

Se recomienda que todos los alimentadores y entradas del servicio eléctrico a las instalaciones se dispongan subterráneamente.

Generación de energía dentro del propio sitio.

Los generadores de respaldo se utilizan para energizar el equipo del centro de datos en caso de que se produzcan fallas en la red eléctrica. Los generadores de emergencia (en contraposición a los de respaldo) se utilizan para potenciar los sistemas de seguridad vitales del centro de datos (por ej., luces de emergencia, bombas de incendios) si se producen fallas en la red eléctrica.

Los generadores de respaldo pueden ser tan pequeños como un auto compacto o tan grande como un camión completo. Algunas soluciones de generadores pueden utilizar un espacio equivalente al de un gran contenedor de carga o incluso mayor. Pueden colocarse en interiores o exteriores y es común que los generadores estén instalados en la azotea de un edificio.

Para que los edificios puedan ocuparse en caso de cortes eléctricos prolongados, las áreas exteriores al centro de datos deben cumplir requisitos básicos de seguridad vital y ocupación, incluyendo, pero sin limitarse a ello, iluminación, alarma contra incendios, baños funcionales, ascensores, sistemas de seguridad y ventilación.

Al seleccionar un sitio, considere el espacio necesario para uno o más generadores de respaldo o de emergencia y sus respectivas vías de circuitos de seguridad vitales y de energía eléctrica. Es preferible que se sitúen en el sitio del centro de datos en una manera segura y conveniente desde un punto de vista estético.

Dentro de las consideraciones de espacio para los generadores también debiera contemplarse el área para bombas de combustible, tuberías y almacenamiento en el sitio. Para algunas aplicaciones del centro de datos, el espacio requerido puede ser bastante costoso pues los requisitos de funcionamiento pueden estipular un rendimiento mínimo de 48 horas sin contar con recursos ni servicios externos. (TIA-942, 2018)

Fase II: Evaluación del Espacio.

2.1 Capacidad General de la Instalación

El termino centro de datos incluye todos los edificios, instalaciones y salas que contienen servidores de empresa, equipos de comunicaciones entre servidores, equipos de refrigeración y equipos de alimentación y que prestan algún tipo de servicio de datos.

El objetivo principal al diseñar la infraestructura para un centro de datos, es proporcionar a los equipos de cómputo el ambiente adecuado para cumplir de la mejor manera las funciones para las que es diseñado, y los requerimientos de especificaciones de los fabricantes del hardware, así como cumplir con los

requisitos de confiabilidad, eficiencia y sustentabilidad exigidos por la comunidad internacional.

2.2 Sistemas de Energía

Cuando se planea el diseño de un centro de datos, muchas veces no se tienen en cuenta el consumo de energía que se va a generar y como se puede optimizar. Muchas veces el costo puede superar el valor de la inversión en equipos e infraestructura en general. (cartagena, 2018)

La electricidad es prioridad para la operatividad de todo el equipo de tecnología, es por ello, que a la hora de realizar el diseño eléctrico se debe contemplar un estudio de carga con un buen nivel de redundancia tanto de un grupo electrógeno como de UPS que garantice el suministro continuo y seguro de la energía eléctrica.

Es de gran importancia evaluar todos los riesgos en las instalaciones eléctricas con el fin de asegurar las personas y el ambiente. Entre las posibles fallas, se encuentra la ausencia de energía, cortocircuitos, rayos, equipos fallando, sobrecarga, entre otros. El sistema eléctrico que se implementa en un centro de cómputo, genera un impacto tanto económico como de disponibilidad de la información en la compañía. Uno de los mayores riesgos que se tiene al momento de instalar un equipo es no contar con un sistema eléctrico adecuado.

El sistema de distribución de energía incluye la energía principal en el centro de datos (o el edificio), los transformadores, paneles de distribución de energía con breakers, el cableado, el sistema de tierra, tomacorrientes, y cualquier generador de energía, suministros de energía u otros dispositivos que se tiene para alimentar de energía al centro de datos.

Un suministro de energía ininterrumpido (UPS) es un componente crítico de alta disponibilidad. En caso de que la energía de la red eléctrica falle, el UPS debe suministrar energía al 100 por ciento del hardware por el tiempo necesario hasta

que se encienda algún generador de respaldo. Debe también llevar 150 por ciento de la carga de energía para complacer condiciones de sobrecarga de falla. También, hay que incluir los requisitos de alimentación necesarios para encender cualquier equipo de emergencia y equipos electrónicos necesarios para acceder al centro de datos, como lectores de la tarjeta de acceso.

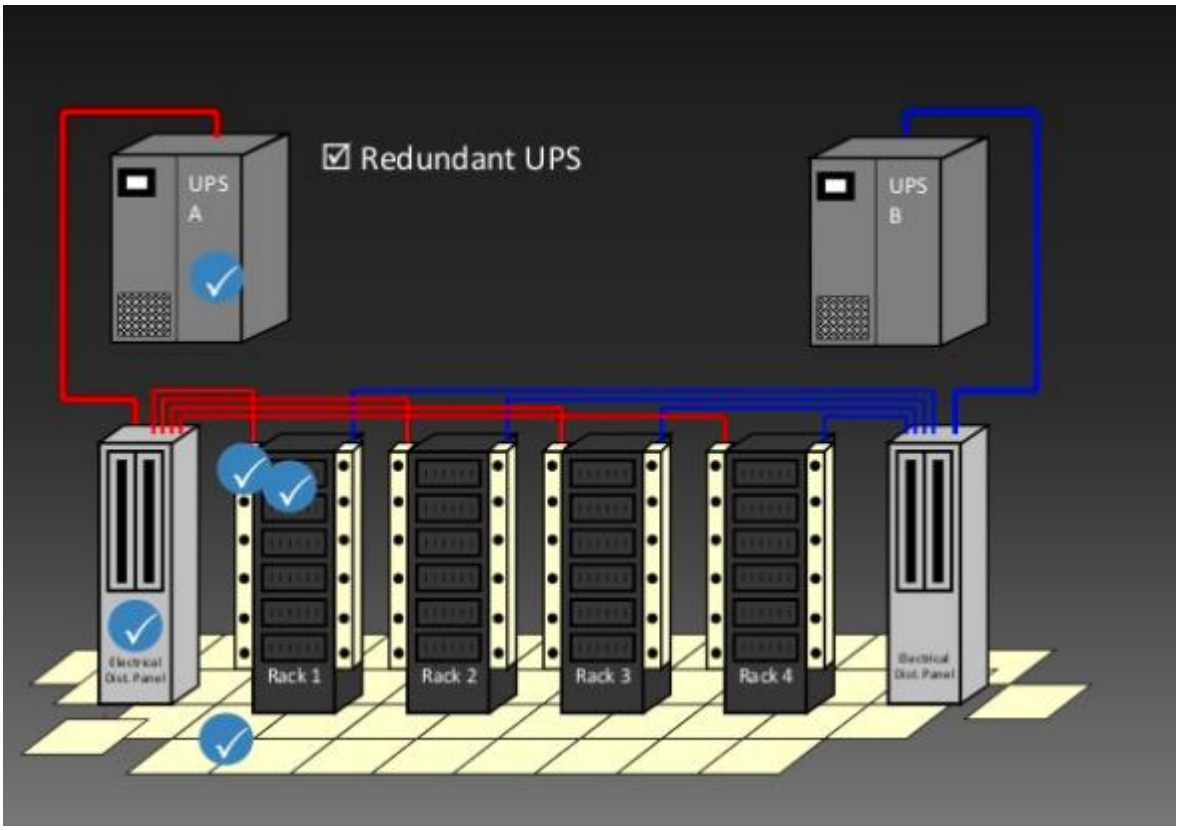


Figura 16. Ups Redundantes

El sistema típico de distribución eléctrica del centro de datos de legado se conforma de cinco componentes.

- La energía se suministra al centro de datos a voltaje medio desde una fuente de energía de servicio público/ generador.
- La energía se baja de voltaje medio a voltaje de distribución (480 V) mediante un transformador de subestación.

- La energía va entonces a través de un sistema de suministro de energía interrumpible (UPS) que acondiciona la energía y proporciona una capacidad de viaje completo durante un apagón hasta que inicie el generador.
- Después, la energía se baja a voltaje de subestación (208/120 V) mediante una unidad de distribución de energía (PDU).
- El PDU suministra energía al suministro de energía de TI, donde se rectifica y se baja hasta 12 Vcd, que es el voltaje de operación interna del equipo de TI. (TIA-942, 2018)

2.3 Capacidad de Climatización.

Unos de los factores vitales en los centros de datos es el acondicionamiento ambiental, pues de acuerdo con un sistema de enfriamiento de los servidores se garantiza un buen funcionamiento y se previene posibles pérdidas monetarias de consideración para el dueño del negocio. Esto implica que el sistema de climatización sea eficiente, cumpla con las exigencias actuales y considere su desempeño corto, mediano y largo plazo.

Además de controlar los accesos y vigilar qué personas acceden a nuestro Centro de Datos, es evidente que los servidores físicos deben tener una temperatura y condiciones.

El rango de temperatura óptimo para un Data Center es entre 17 °C y 21 °C. Es necesario aclarar que esa temperatura no es de carácter obligatorio, sino que existe también un margen aceptable de operación que sería de 15 °C y 25 °C. Cualquier temperatura mayor a 25 °C deberá ser corregida de manera inmediata, ya que implica poner en riesgo el equipamiento del Data Center.

En 2004 la recomendación de operación era entre 20 °C y 25 °C; en la publicación del año 2008, el rango recomendado se amplió a 18 °C y 27 °C. En el año 2011, el rango recomendado se mantuvo, pero se amplió el rango permitido de 5 °C a 40

°C (cabe aclarar que esto no es para todos los tipos de Data Centers, sino que varía según su clasificación). El principal impulsor para ampliar los límites provino de la necesidad de la industria de tener mayor flexibilidad, y al mismo tiempo, de reducir costos en enfriamiento, para lo cual se debe tener un claro conocimiento de la edad de los servidores y su política de renovación. No es lo mismo renovar los equipos cada tres, cinco o siete años, si bien cuando se compran los equipos nadie lo hace pensando que van durar 10 años; en la práctica termina siendo mucho más habitual de lo que creemos, ya sea por razones presupuestarias o dificultades de migración.

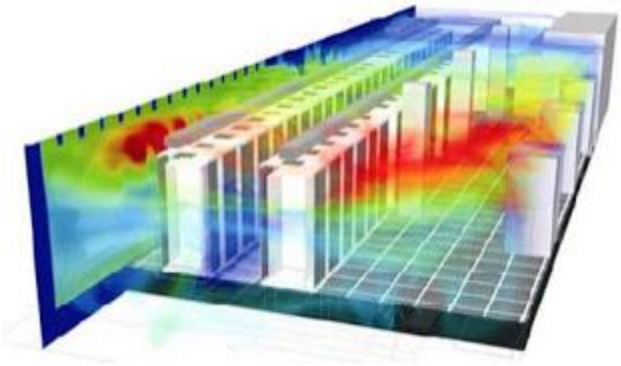


Figura 17: Enfriamiento de un centro de Datos.

Si sabemos que nuestros equipo si sabemos que nuestros equipos se renuevan siempre cada tres años probablemente no tengamos problemas operando nuestro Data Center a 27 °C. En cambio, si sabemos que la vida útil de nuestros servidores va a ser mucho más extendida, deberíamos pensar en un rango de operación más bajo para así prolongar la duración de los equipos. Como se citó anteriormente, según la Regla de los 10 grados, a menor temperatura, mayor es la durabilidad de los componentes. (TIA-942, 2018)

Por otra parte la norma TIA/EIA-942 recomienda como rango aceptable de temperatura entre 20 °C y 25°C. Se renuevan siempre cada tres años probablemente no tengamos problemas operando nuestro Data Center a 27 °C. En cambio, si sabemos que la vida útil de nuestros servidores va a ser mucho más

extendida, deberíamos pensar en un rango de operación más bajo para así prolongar la duración de los equipos. Como se citó anteriormente, según la Regla de los 10 grados, a menor temperatura, mayor es la durabilidad de los componentes por otra parte la norma TIA/EIA-942 recomienda como rango aceptable de temperatura entre 20 °C y 25 °C.

El rango que recomiendan las empresas fabricantes de servidores:
BM: 22 °C, Dell: 23 °C, HP: 22 °C

2.4 Espacios que complementan el Centro de Datos

Un centro de datos dispone de espacios de uso exclusivo donde las empresas mantienen y operan sus infraestructuras IT. Es ese espacio donde se pueden alojar los servidores y sistemas de almacenamiento para ejecutar las aplicaciones que procesan y almacenan datos de empresas. Algunas empresas disponen de una Jaula o de solo uno o varios racks (bastidor), mientras que otras pueden disponer de salas privadas para alojar un número determinado de armarios rack, dependiendo del tamaño de la empresa.

El centro de datos proporciona el espacio técnico preparado con falso suelo por debajo de cual se instalan la toma eléctrica para conectar los bastidores.

El control de clima para mantener unos parámetros de temperatura y humedad correctos que garanticen el correcto funcionamiento y la integridad operativa de los sistemas alojados. Los centros de datos cuentan con sistemas de alimentación eléctrica, alimentación de reserva, refrigeración, cableado, detección y extinción de incendios, detectores de fugas de agua y controles de seguridad.

Un Datacenter físico puede alojar centro de datos virtuales, conocidos como cloud centro de datos o cloud privado, con un menor coste gracias a la capa de virtualización. Cada Centro de datos virtual es totalmente independiente de otros,

por lo que, cuenta con las máximas garantías de seguridad, disponibilidad y flexibilidad. (TIA-942, 2018)

2.5 Arquitectura de red

El cableado de red es muy importante al momento de poner en marcha el centro de datos. Es importante determinar las opciones en cables, cuántas conexiones se proveerán, y como estarán organizadas las terminaciones. Algunos pasos a tener en cuenta son:

- Tender el cable en las instalaciones al momento de la construcción o levantamiento del centro de datos.
- Utilizar cables lo más corto posibles en la medida que se pueda
- Escoger el cable adecuado para cada conexión.

- Paneles de rendimiento (Patch Panel)

Los llamados Patch Panel o paneles de rendimiento son utilizados en algún punto de una red informática donde todos los cables de red terminan. Se puede definir como paneles donde se ubican los puertos de una red, normalmente localizados en un rack para red. Todas las líneas de entrada y salida de los equipos (ordenadores, servidores, impresoras, etc.) tendrán su conexión a uno de estos paneles.

Los Patch Panel permitirán hacer cambios de forma rápida y sencilla conectando y desconectando los cables. Esta manipulación de los cables se hará habitualmente en la parte frontal, mientras que la parte posterior del panel tendrá los cables más permanentes y que van directamente a los equipos centrales. La distancia máxima permitida entre el puesto de trabajo y el armario de distribuciones o dispositivo de interconexión es de 100 mts. (TI, 2018)

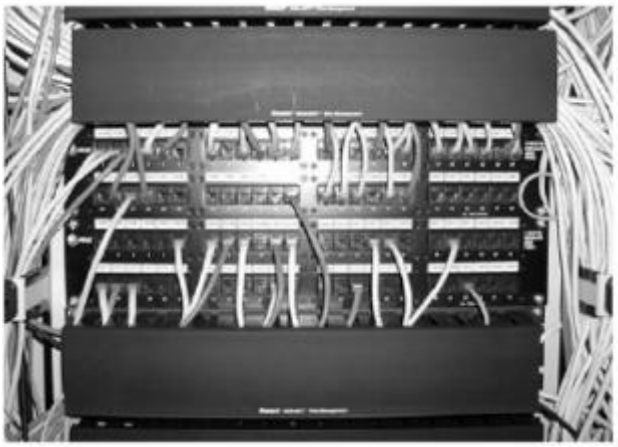


Figura 18: sistema de cableado

Conectores de Cable

El conector RJ - 45 es el estándar para el cableado de cobre categoría 5e. Sin embargo, el cable de fibra tiene algunas opciones: Tipo de conector LC, SC, y ST.

Figura 19: Tipos de cables

- Evitar Cables Enredados

No es bueno en un centro de datos los cables enredados. Se debe tomar las siguientes recomendaciones:

1. Usar la longitud correcta de Cat5e, o 6e, o cables de fibra qué vaya de punto a punto.
2. Encaminar cables, cuando sea posible, bajo los paneles de los pisos levantados.
3. Etiquete cada cable a ambos puntas.
4. Evitar el direccionamiento de cable sobre el piso.

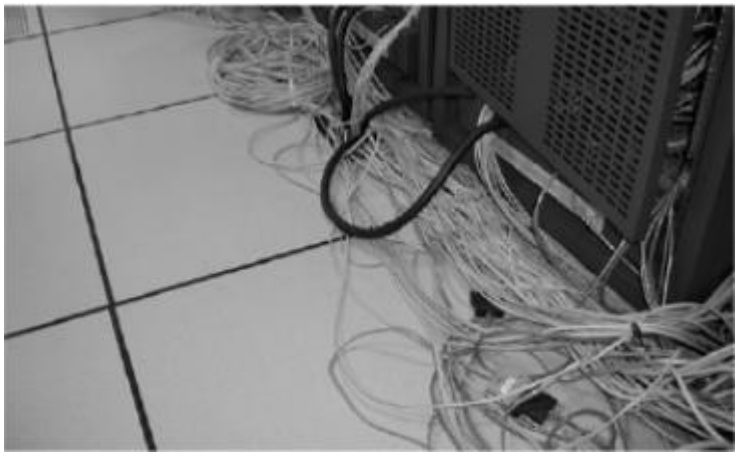


Figura 20: Cables desorganizados

2.6 Etiquetado y codificación de color

Se etiquetan las entradas en los Patch panel, pero también se debe etiquetar los cables, y en ambas puntas. Si una máquina está teniendo problemas de conectividad de la red, puede determinar qué cable y puerto están fallando.

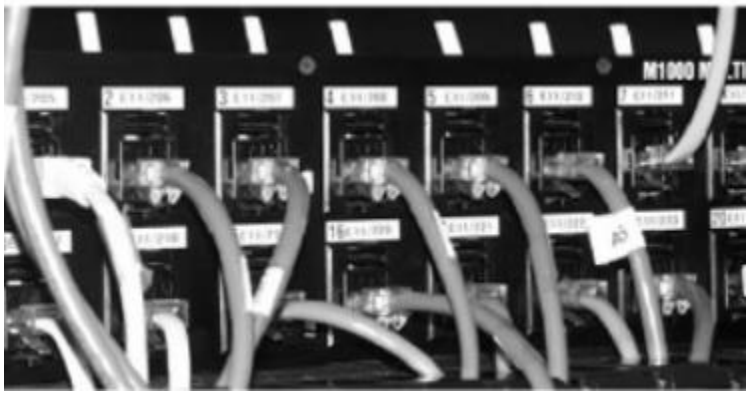


Figura 21: Cables organizados y etiquetados

Clasificar los cables por colores es también útil, si no se puede usar cables de diferentes colores, se puede usar etiquetas codificadas por colores sobre los cables. (TI, 2018)

Fase III: Evaluación Arquitectónica.

3.1 Planificación de instalaciones

"Un Data Center se construye con los mejores materiales y las mejores prácticas." El proceso de selección del sitio supone un paso crucial a la hora de reducir los riesgos vinculados a un centro de datos, muchos de los centros de datos se han construido con los más elevados niveles de disponibilidad, pero en lugares equivocados. Una mala elección del sitio puede tener un alto impacto en la clasificación de disponibilidad general de las instalaciones. Las decisiones relativas a la selección del sitio deben tener en cuenta:

- Riesgos ambientales
- Riesgos físicos
- Suministro de servicios
- Crecimiento futuro
- Vecinos, tanto actuales como futuros.

Es importante tomar en cuenta las recomendaciones realizadas por las normas y estándares internacionales, ya que disponen de una serie de criterios para la elección de los sitios y que incluyen distancias recomendadas de separación a diversos peligros identificados. Estas recomendaciones deberían ser consideradas en el momento de acometer el proceso de análisis de riesgos para los distintos lugares. (BICSI, 2018)

3.2 Conceptos generales de diseño

El tipo de estructura vendrá marcado por la ubicación y los códigos de construcción locales que a su vez tendrán en cuentas las condiciones ambientales locales y los materiales de construcción para resistir vientos, movimientos sísmicos e inundaciones. La adecuación de la estructura exterior para su uso como centro de datos será determinada por varios factores, por ejemplo: capacidad de carga desde el techo, tamaño y ubicación de los pilares o columnas internas, tipo de construcción del techo, alturas mínimas tomando en consideración el piso falso.

En el diseño arquitectónico es importante considerar las consideraciones de espacio entre los diferentes cuartos y salas que conforman el centro de datos:

- Sala informática
- Cuarto eléctrico
- Zona de soporte
- Zona exterior

Así mismo se debe de tomar en cuenta los elementos de diseño importante sobre el edificio:

- Dimensiones y forma de la sala
- Carga en el suelo
- Resistencia al fuego
- Entradas y salidas
- Iluminación

- Seguridad
- Suelo técnico o piso falso
- Disposición del techo
- Supresión de fuego (BICSI, 2018)

Los requisitos de espacio de la sala informática se derivan de la evaluación de necesidades de negocio, que permitan crecimiento futuro en base a la cantidad y tamaño de equipo, contar con un espacio adecuado para la infraestructura de cableado y tener una forma regular para maximizar el aprovechamiento del espacio.

Obra Civil: Los muros perimetrales del ambiente de tecnología de la información deberán ser hechos con materiales sólidos y permanentes, deberán ser construidos de techo a piso. Deberá ser hermético que garantice la impermeabilidad y resistencia sísmica de la clasificación sísmica que corresponda al lugar de estación, deberá impedir la propagación de humos, vapores, humedad y polvo hacia el interior, transmisión de calor exterior hacia el interior del centro de datos. Se deberá considerar el nivel de seguridad requerido para el caso de vandalismo, sabotaje y terrorismo, así como ataques con armas de fuego, deberán tomarse las medidas necesarias para evitar que la interferencia electromagnética exterior afecte los equipos de cómputo. En caso que el diseño arquitectónico requiera de la utilización de cristales, estos deberán ser templados, resistentes al impacto e inastillables con un espesor mínimo de 9mm, pero nunca podrán formar parte del perímetro exterior del centro de datos. Los muros no podrán ser materiales con relleno que sea inflamable y/o produzca humos tóxicos. (BICSI, 2018)

3.3 Vías generales de acceso

Un centro de datos debe de contar con la facilidad de acceso (pues hay que meter en él aires acondicionados pesados, muebles de servidores grandes, etc.)

El cuarto debe ser completamente cerrado; es decir, los rayos solares no deben entrar al cuarto de cómputo, por lo que se recomienda la no utilización de ventanas.

Rampa de acceso Se debe proveer un medio de acceso al piso técnico. Este acceso no debe tener una inclinación mayor a 13 grados equivalentes a una pendiente de 21% y deberá estar cubierto por material anti-derrapante y estar provisto de pasamanos.

- Puerta de acceso a equipos dentro del Centro de datos.

La dimensión de la puerta de acceso para equipos deberá ser 1.10 m de ancho libre como mínimo y 2.30 m de altura libre si es de una sola hoja y de 1.80 m de ancho y 2.30 m de altura si es de doble hoja. Deberá contar con un mecanismo de cerrado automático y abatir hacia afuera del ambiente de tecnologías de la información.

- Puertas. Puerta de acceso al personal.

La dimensión del claro de acceso principal deber ser 0.90 m como mínimo y deberá ser de material no combustible. Deberá contar con un mecanismo de cerrado automático y abatir hacia afuera del ambiente de tecnologías de la información.

- Puertas de Emergencia.

La puerta de salida para emergencia deberá tener una barra anti pánico hecha de material no combustible, su posición deberá ser opuesta al acceso principal, deberá contar la señalización correspondiente y marcar claramente la ruta de evacuación, deberá abatir hacia afuera del ambiente de tecnologías de la información. No deberán dar hacia el exterior del inmueble ni hacia pasillos de evacuación del inmueble, no deberán tener cerraduras ni candados. Deberá ser de un ancho libre mínimo de 1.10 m y una altura libre de 2.30 m, así como contar con un dispositivo sonoro que indique que la puerta ha sido abierta y se restablezca manualmente. (TIA-942, 2018)

3.4 Detalles de planificación

Uno de los primeros factores en los que deben fijar la atención es saber qué tipo de centro de datos quieren tener. No todos los centros de datos son iguales. Los centros de almacenamiento de datos se clasifican según el Tier al cual pertenecen y según el tipo de actividad que efectuarán durante su operación.

- **Equipamiento:** El nivel de equipamiento con el que cuente el centro de datos depende mucho de las funciones que vaya a realizar y de las necesidades de la empresa. Así que debes pensar en implementar los equipos informáticos necesarios para su buen funcionamiento, desde los servidores hasta los sensores y cámaras de seguridad.

- **Climatización:** Uno de los aspectos preventivos más importantes para un centro de datos consiste en mantener la temperatura y humedad de la sala en donde se instalará. Así que para evitar daños en los equipos, incidentes que pongan en riesgo la operación e información de la empresa o, en peores casos, incendios. Es vital contemplar la instalación de sistemas de climatización.

- **Consumo energético:** Otro de los aspectos a evaluar es el consumo eléctrico del centro de datos. Hacer un análisis de los equipos secundarios como aires acondicionados de precisión, iluminación, entre otros, para determinar el consumo total eléctrico del centro de datos.

- **Conectividad y red:** El cableado y una red integral harán que el sistema del centro de datos tenga un funcionamiento operacional constante y libre de riesgos. Este es un aspecto fundamental porque una correcta operación en este sentido permitirá que el acceso a la información de la empresa y el rendimiento de tus equipos de trabajo sea fluido y sin interrupciones.

- **Sistemas de seguridad:** La información es uno de los activos más importantes. El compromiso con el cuidado de los datos y equipos debe ser máximo, debido a esto,

se vuelve imprescindible el uso de equipos de control y sistemas de seguridad avanzados que limiten el acceso de personal a esta área de la empresa.
(TIA-942, 2018)

Fase IV: Evaluación del Sistema Eléctrico

4.1 Descripción general

El centro de datos debe contar con circuitos dedicados al mismo con centros de carga alimentando cada espacio. Se instala contactos dúplex (127V/20Amp) cada 3.5 m en las paredes para uso general. Los circuitos para los contactos se conectan a centros de carga separados en el centro de datos.

El sistema eléctrico de un centro de datos debe contar con al menos un Sistema de Energía Interrumpible (UPS) y una planta de emergencia (generador) dedicados al mismo.

N+1 o Tier 2: Debe de contar con dos UPS´s con tecnología doble conversión en configuración paralelo redundante o redundante aislado con capacidad del 100% de la carga y redundancia al 100%, conectados a una planta de emergencia exclusiva para el centro de datos.

Se debe de contar un sistema de monitoreo es recomendado para el (los) UPS y la(s) planta(s) de emergencia.

4.2 Servicio de red eléctrica

Se deberá de tomar en cuenta la ubicación del centro de datos para que cuente con el flujo de energía eléctrico necesario para asegurar con el funcionamiento de todos los equipos, independientemente de las condiciones externas ya que el centro de datos tiene que seguir funcionando sin interrupción de manera transparente para los usuarios.

Se debe de contar con un método de contingencia de energía eléctrica para que los equipos de misión crítica cuenten con la alimentación adecuada de energía.

4.3 Distribución

El sistema típico de distribución eléctrica del centro de datos de legado se conforma de cinco componentes. La energía se suministra al centro de datos a voltaje medio desde una fuente de energía de servicio público/ generador. La energía se baja de voltaje medio a voltaje de distribución (480 V) mediante un transformador de subestación.

La energía va entonces a través de un sistema de suministro de energía interrumpible (UPS) que acondiciona la energía y proporciona una capacidad de viaje completo durante un apagón hasta que inicie el generador. Después, la energía se baja a voltaje de subestación (208/120 V) mediante una unidad de distribución de energía (PDU).

El PDU suministra energía al suministro de energía de TI, donde se rectifica y se baja hasta 12 Vcd, que es el voltaje de operación interna del equipo de TI.
(schneider-electric, 2018)

4.4 Sistemas de suministro de energía ininterrumpida (UPS)

Los sistemas interrumpibles de energía son a la vez excelentes filtros de anomalías, equipos que permiten que los consumos no se enteren que se ha producido un corte del suministro eléctrico, ya que tiene la propiedad de seguir alimentando a los consumos a través de un sistema de baterías incorporado. El tiempo que continúe el UPS. Alimentando a los consumos dependerá evidentemente de la capacidad de energía almacenada en las baterías. De esta forma es claro que los UPS. Han superado por lejos a los simples estabilizadores y de esta forma son los únicos

equipos que pueden garantizar que sus equipos no se dañen y puedan seguir operando sin importar que problemas puedan existir en la red eléctrica.
(TIA-942, 2018)

Un centro de datos debe de contar un sistema que controle las caídas constantes de energía y evite la interrupción del enfriamiento. Para esto, se debe de implementar componentes como UPS. (Institute, 2018)

Si se produce un corte de energía, en ese momento, la unidad de control detecta la ausencia de suministro y el sistema continúa trabajando a través de la energía que provee las baterías que se mantenían cargadas gracias al cargador o rectificador. Vale decir que los consumos continúan trabajando gracias a que el inversor está convirtiendo la energía continua de las baterías en energía alterna y los consumos ni se enteran, porque nunca existió un corte de energía en sus entradas o fue muy pequeño del orden de los milisegundos suficiente para que no sea percibido por los mismos. Ese tiempo de corte se lo denomina tiempo de transferencia y dependiendo del tipo de UPS. Este tiempo puede llegar a ser nulo, como lo mencionamos. (TIA-942, 2018)

4.5 Sistemas de energía de reserva y emergencia.

Un elemento muy crítico suele ser el sistema de alimentación de energía eléctrica lo que debe d atenerse en cuenta a la hora de planificar la instalación. Lo más común debe de ser dotarla de un sistema de alimentación interrumpida (UPS) que proteja durante la caída de tención o durante las oscilaciones de la misma. Estos sistemas suelen estar apoyados en un grupo de baterías de reserva que entra en servicio ante el fallo de alimentación principal de corriente alterna manteniendo el servicio hasta que se restablezca las condiciones iniciales.

También se debe de contar con una planta eléctrica alterna, las oficinas regularmente pierden la electricidad durante corto o largo periodo de tiempo. Para

evitar esos largos periodos de corte se necesita una planta eléctrica que Trabaje con base a algún combustible. Conforme las necesidades de electricidad aumenten así deberá ser la capacidad de la planta eléctrica.

4.6 Iluminación

Se debe de contar con lámparas fluorescentes de alta eficiencia, fabricados de acero galvanizado con bases de porta tubos de policarbonato con seguro y dispensar de temperatura con tubos fluorescentes 18 w color blanco frio.

- Alumbrado de emergencia

Se facilitará a la sala un alumbrado de emergencia de 5 lúmenes/m2 y autonomía de 60 minutos y baterías recargables libres de mantenimiento con tiempo de recarga de 4 horas.

Habrá una indicación encima de las puertas en el interior de la sala de “Salida de Emergencia”, su disposición será tal que entre las filas de equipos sea fácilmente distinguible el alumbrado facilitando con ello la evacuación de la sala en caso de riesgo. (schneider-electric, 2018)

4.7 Uniones, puesta a tierra, protección contra rayos y supresión de sobre voltajes

La unión a tierra permite que muchos dispositivos de cableado se interconecten con el sistema de conexión a tierra.

Con una buena instalación de la unión y de la conexión a tierra se logra lo siguiente:

- Se minimiza los sobre voltajes y picos de electricidad.
- Mantener la integridad de la planta de conexión a tierra eléctrica.

- Lograr una vía más segura y efectiva de conexión a tierra.

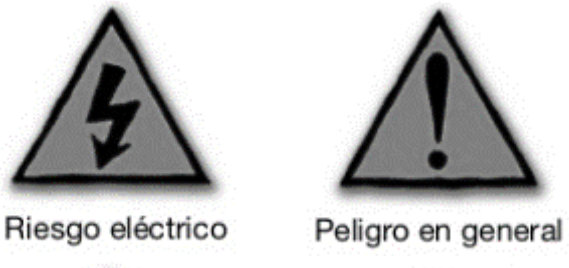
Los aterramientos para los sistemas de telecomunicaciones parten del aterramiento principal del edificio (aterramiento eléctrico, jabalinas, etc.). Desde ese punto, se debe de tener un conductor de tierra para telecomunicaciones hasta la barra principal de tierra para telecomunicaciones.

Este conductor a tierra debe de estar forrado preferentemente de color verde y debe tener una sección mínima de 6 AWG se recomienda que el conductor de tierra no sea ubicado dentro de canalizaciones metálicas, estas deben estar eléctricamente conectadas al conductor a tierra de ambos extremos. (schneider-electric, 2018)

Figura 22: Cables de conexión a tierra

4.8 Etiquetas y señalética

El conjunto de señales y símbolos tienen una función de guiar, orientar y organizar a una persona o conjunto de personas hacia un destino. Se debe de utilizar la señalética como vehículo importante de identidad corporativa.



(schneider-electric, 2018)

Fase V: Evaluación del Sistema Mecánico

5.1 Tecnologías típicas de enfriamiento para la sala de computadoras y de rechazo térmico.

Se recomiendan las siguientes tecnologías de equipo de refrigeración:

- **Aire acondicionado de precisión:** Estos equipos son especiales para mantener una temperatura y humidad muy precisas.

- **Unidades de aire tipo Closely coupled cooling:** Estas unidades enfrían áreas específicas, como un pasillo, un rack o un servidor, desde una distancia cercana, de modo que se le mezcla el aire frio con el caliente y las trayectorias de aires son más cortas.

- **Tecnologías de compresores como digital scroll compressors:** Estos equipos posibilitan altas eficiencias en cargas parciales de centros de datos. (BICSI, 2018)

Figura 23: Unidad de aire acondicionado de precisión

5.2 Condiciones ambientales

El correcto funcionamiento de los centros de datos pasa por mantener un adecuado equilibrio en sus condiciones ambientales.

La calve se sitúa en mantener unas condiciones óptimas para que los equipos puedan trabajar en las mejores condiciones, mantener controlada las instalaciones mediante los sistemas de control ambiental.

Si hablamos de temperatura ambiental la situación ambiental se mantiene entre los 21 y 23 grados Celsius. Los equipos pueden trabajar con una franja de temperatura amplia, para mantener la temperatura cercana a los 22 grados Celsius la cual proporciona varias ventajas: mayor fiabilidad de los sistemas y contamos con un pequeño margen de seguridad en caso de que fallen los sistemas de control ambiental.

Hablando de humedad, situar la humedad relativa ambiente entre un 45 y 50% nos garantiza el correcto funcionamiento de los equipos. Nos ayuda a prevenir posibles problemas de corrosión por niveles de humedad bajos, así mismo se disminuye el riego de descargas estáticas y electroestáticas y nos da un poco más de tiempo ante un posible fallo del sistema de control ambiental.

Los sistemas de control ambiental inalámbrico o por cableado nos ayudan a controlar las condiciones de temperatura, flujo, aire, ruido, intensidad de la luz, humedad, presencia de líquidos, entre otros a través de sensores. Estos sistemas informan mediante portal web, correo o cualquier sistema colector. Además se puede acceder a los sistemas a la información ambiental al momento a través de un ordenar o Smartphone.

Estos dispositivos cuentan con un hub interno de puertos seriales que permiten ir incorporando más sensores si es necesario, de tal forma que pueden crecer de forma escalonada y con una inversión progresiva. (BICSI, 2018)

5.3 Administración térmica

La administración térmica de un centro de datos brinda una evaluación básica de la efectividad del sistema de refrigeración. Utilizando las mejores prácticas de la infraestructura física de refrigeración.

El acomodo de los equipos es importante de lo contario se pueden presentar distribuciones de temperatura homogénea.

Se deben de implementar técnicas de acomodo de equipos, se debe de dividir los pasillos en fríos y calientes de manera que los aires acondicionados depositen aire frio en los pasillos fríos y recogen el aire caliente de los pasillos calientes.

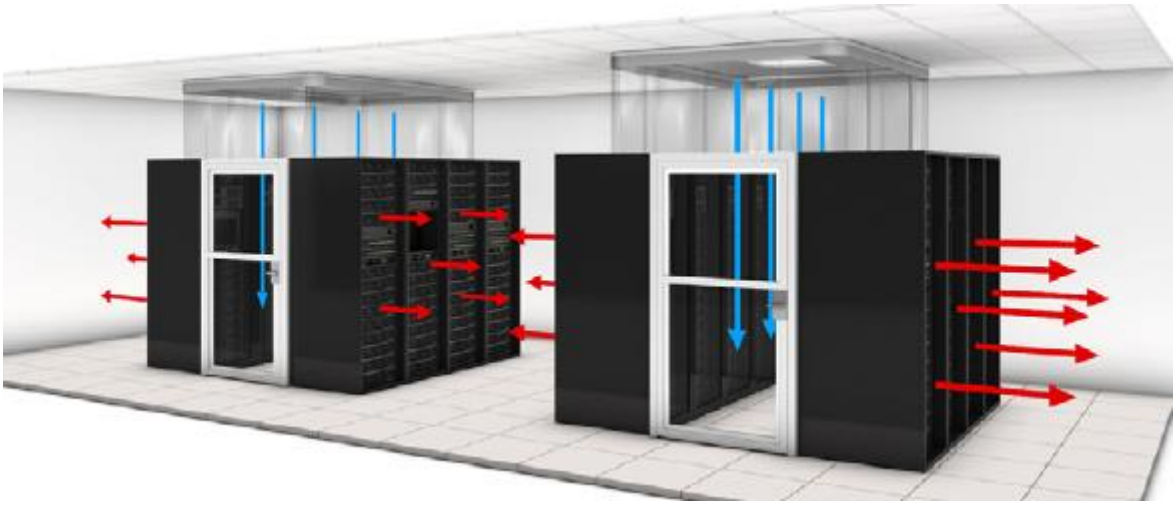


Figura 24: Técnica de dividir pasillos fríos y calientes

Fase VI: Evaluación de la Protección contra incendios

6.1 Paredes, pisos y cielos rasos

- Pisos Falsos:

Se debe instalar un piso falso modular y removible. Deberá de ser construidos con materiales no combustibles, soportar una carga de 450 kg colocado al centro del módulo. La altura libre entre piso real y piso falso (Plenum de piso), debe de ser 30 cm como mínimo. En construcciones nuevas se debe de contemplar 60 cm libres como mínimo.

No deberá de estar fabricados de láminas “Electro-Plateadas o galvanizadas” que producen un efecto “Zinc whiskers” (Emisión de partículas mecánicas de zinc) en la unión entre piso y pared se deberá de colocar la cinta de sellado de 10 cm para evitar la fuga de aire perimetral.

Todos los cortes deberán de quedar totalmente cubiertos con hule o material similar, de tal forma que los filos de las láminas no queden expuestos y evitar así el daño a los forros de los cables que pasen por ahí y el efecto Zinc whiskers” (Emisión de partículas mecánicas de zinc)
(Norma NFPA 76, 2018)

- **Cielos rasos:**

Debe de contar con una superficie instalada de 120m2, cielo de placa de fibra, térmico estable ignifugo, acústico.

- **Paredes:**

Usar láminas de fibra de vidrio para aislamiento térmico y acústico en las paredes simplifica considerablemente la obra civil, las bondades del gypsum se aprovechan de mejor manera y su instalación es más limpia.

Se debe emplear pintura látex vinílico y se deben aplicar dos manos. Deberá de ser de color claro.

6.2 Contención de pasillos

La contención de pasillos previene la mescla de aire frio con aire caliente dentro del centro de datos. Esto permite que el retorno de aire hacia el equipo haga una temperatura más alta mejorando la eficiencia del sistema de enfriamiento, reduciendo los costos de energía.

Se recomiendo el uso de soluciones de contención de pasillos calientes por varios motivos.

Al concentra el aire caliente las unidades de refrigeración se mantienen en zonas optimas de trabajo. El aire frio expulsado a los pasillos fríos puede ser utilizado para bajar la temperatura total de la sala. Mejorando el consumo de energía. (NFPA, 2018)

6.3 Extintores manuales de incendios

En cuanto a medios manuales se debe de contar con bocas de incendios equipadas, extintores portátiles preferiblemente por gas en la sala (Dióxido de carbono son las más comunes aunque en la actualidad hay disponibles de otros agentes limpios) e hídricos en aquellas zonas donde pueda haber papel o combustible ordinarios. Los extintores de polvo se desaconsejan en las salas.
(TIA-942, 2018)

Figura 25: Extintor de Dióxido de carbono

6.4 Protección contra incendios

El NFPA 75 es el estándar para la protección contra incendios de equipos de tecnología de la información, se centra en los centros de datos. (NFPA, 2018)

El propósito de la NFPA 75 es el de establecer los requisitos mínimos para la protección del equipamiento de tecnología de la información y de las áreas para los equipos de tecnología de la información, de los daños ocasionados por el fuego.
Deben contener cerramientos con clasificación de resistencia al fuego y las aberturas deberán estar protegidas para restringir la propagación de fuego y para restringir el movimiento de humo. (NFPA, 2018)

Estas áreas deberán contar con un sistema de rociadores automáticos, un sistema de extinción de agente limpio, o ambos; para reducir al mínimo los daños a los equipos electrónicos de los computadores localizados en las áreas protegidas con rociadores, es importante que se haya desconectado la energía antes de aplicar agua sobre el fuego. (NFPA, 2018)

Este nivel de protección requiere de ciertos criterios de diseño, por ejemplo, cierre de las compuertas cortafuego, desconexión de equipos suministradores de aire de precisión, entre otros con el fin de garantizar que se logrará la concentración requerida para la extinción del fuego.
(NFPA, 2018)

6.5 Detección de incendios

Es de vital importancia contar con un sistema de detección de incendios según la norma NFPA 76 se debe de contar con los siguientes sistemas:

EWFD: sistema que usan humo, calor o flama para dar alerta temprano de fuego.

Figura 26: Sistema de detección EWFD

VEWFD: Sistema que detecta fuego de baja energía antes que sean una amenaza para las instalaciones. (Norma NFPA 76, 2018)

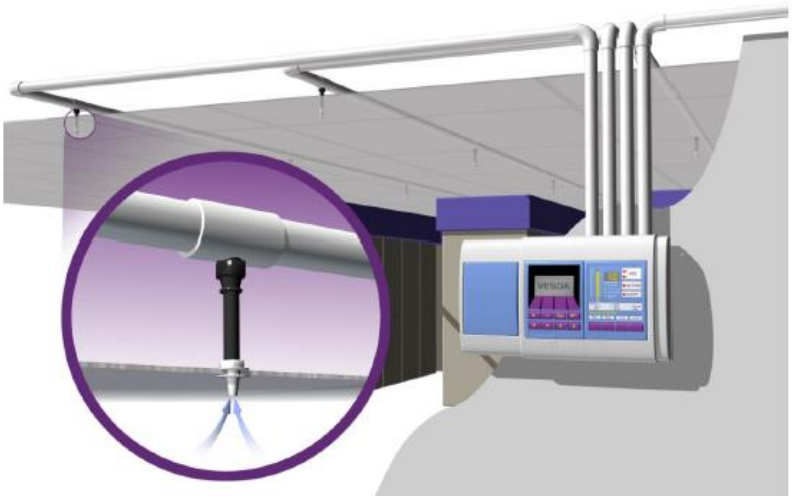


Figura 27: Sistema de detección de incendios VEWFD

6.6Etiquetas y señalética

Fase VII: Evaluación de la Seguridad

7.1 Generalidades

Actualmente existen estándares, protocolos, métodos y reglas que permiten minimizar riesgos a la infraestructura o información. La seguridad abarca software, bases de datos, metadatos, archivos y todo lo que la organización valore como activo y signifique un riesgo es decir en cuanto al tipo de información que se conoce como privilegiada o confidencial. (TI, 2018)

7.2 Plan de seguridad física

La seguridad física de los centros de datos implica proteger la infraestructura crítica de amenazas externas o intrusiones que atenten contra las actividades de una empresa. Elementos de alto valor o sumamente importantes tales como servidores, switches y unidades de almacenamiento.

De acuerdo al centro de seguridad nacional,(National Computer Science Center), la seguridad física que se debe de aplicar a un centro de datos, se define como la aplicación de barreras físicas y el control de procedimientos como medidas preventivas contra la amenaza a los recursos y a la información sensible.
(normas aplicadas pragon, 2018)

La seguridad física es uno de los puntos más importantes a la hora de diseñar la infraestructura física.

- **Control de acceso:**
  En especial en las zonas “cero” es decir aquellos compartimientos del centro de datos que albergan la infraestructura más valiosa. Se debe de tener un control en tiempo real de quien entra a donde y para qué. Instalan sistemas biométricos y siguen siendo válidos los mecanismos de acceso con tarjetas inteligentes.

- **Pruebas de mecanismos de detección de alarma:**

  Todos los responsables de seguridad física deben de contar con extintores, sala de contra incendios los sensores de humedad, de temperatura de detección de humo, y de movimiento que debe de ser probados regularmente y que funciones como es debido.

- **Seguridad perimetral:**

  Para garantizar la seguridad perimetral del centro de datos, se debe de tener en cuenta la construcción de toda la tabiquería perimetral utilizando materiales ignífugos con una protección del fuego de al menos 120 minutos.

  Del mismo modo las puertas de acceso al centro de datos deben cumplir los mismos estándares que el cerramiento perimetral.

  Imprescindible para la adecuada gestión del intrusismo dentro del centro de datos es la instalación de un sistema de Control de Accesos que nos permita seleccionar al personal con atributos para su acceso, así como generar un historial que nos permita conocer los eventos relacionados con el acceso al centro de datos. Desde los sistemas de teclado manual, pasando por tarjetas, detección de huella o identificación por retina son sistemas que se pueden instalar para la seguridad perimetral.(TIA-942, 2018)

7.3 Evaluación de riesgos y amenazas

La mayoría de los riegos de entorno serán naturales, tales como: Inundaciones: las zonas inundables no son buena zonas para un centro de datos. Zonas de riesgos sísmicos: cercanas a la costa y baja altitud. Zonas propensas a tornados, tifones, etc.

- **Fugas de líquidos**:
  Evitar conducciones de agua alrededor o en el centro de datos.

- **Temperatura:**

  Se debe de tener capacidad de refrigeración aprovechar en la medida de lo posible las posibilidades que nos del medio ambiente exterior. Tener planes de apagado y emergencia para el caso que se pierda parte o toda la capacidad de refrigeración.

- **Errores humanos:**

  Unas de las principales amenazas de un centro de datos son sus operadores. No es rara la típica operación de mantenimiento rutinaria consistente en conmutación a ups o generadores que terminar en un pagado no programado de la instalación.

- **Contaminación de aire:**
  Se debe de evitar la presencia de polvo o contaminación masiva.

- **Humedad:**
  Humedad excesiva puede generar aparición de corrientes estáticas siendo nocivas para el centro de datos.

- **Suministro eléctrico:**
  Aunque nuestro centro de datos este perfectamente dimensionado, tengamos UPS, generadores, etc. La realidad que no es provisor, quizás el fallo venga de la empresa proveedora del suministro.(TIA-942, 2018)

7.4 Prevención de delitos mediante diseño ambiental

La prevención de delitos a través del diseño ambiental consiste en el diseño, el mantenimiento y el uso del ambiente construido con la finalidad de mejorar la calidad de vida y disminuir la incidencia de delitos y el temor a la delincuencia.

Visibilidad natural: La visibilidad natural se logra a través de un diseño y de un mantenimiento que permiten que las personas que desempeñan sus actividades acostumbradas puedan observar fácilmente el espacio que las rodea, así como eliminar los lugares en los que puedan ocultarse los delincuentes. Por lo general, se logra la visibilidad natural mediante el uso de iluminación adecuada, cercas o elementos de jardinería ornamental bajos o a través de los que se pueda ver, la remoción de áreas que ofrezcan donde ocultarse y la colocación de ventanas, puertas y caminos para transeúntes que permitan que los usuarios responsables de la propiedad puedan observar fácilmente las áreas circundantes.

Territorialidad: Territorialidad significa proporcionar una demarcación clara entre las áreas públicas, las privadas y las semiprivadas y ayuda a que las personas entiendan más fácilmente el uso propuesto del área y la utilicen debidamente. La territorialidad expresa un sentimiento de “propiedad” activa del área que puede desvirtuar la percepción de que pueden cometerse actos ilegales en el área sin que nadie se dé cuenta y sin enfrentar consecuencias. El uso de pantallas (mallas metálicas) traslúcidas, cercas y rejas bajas, letreros y aceras de texturas diversas o de otros elementos de jardinería ornamental que muestren la transición entre las áreas propuestas para usos diversos son ejemplos del principio de territorialidad.

Control del acceso:

El control del acceso es un concepto encaminado principalmente a disminuir la accesibilidad delictiva, sobre todo a áreas en las que no podría verse fácilmente a la persona que se propone cometer un delito. (TIA-942, 2018)

7.5 Alarmas

Todas las puertas exteriores deben contar con alarmas y monitorizarse mediante un circuito cerrado de televisión, de igual manera deben abrirse hacia afuera para favorecer la evacuación en caso de incendio y aumentar la seguridad. (TIA-942, 2018)

7.6 Control de acceso

El control de acceso es un sistema electrónico a través el cual se controla las entradas, salidas y adonde entra cada individuo.

Los componentes más importantes de control de acceso que debe de poseer un centro de datos son:

- Lectoras y tarjetas: Son los dispositivos que deben censar el tipo de información presentada en forma de tarjeta para ingresar o salir de algún lugar donde esté presente este dispositivo.

- Lectora biométrica : Con este tipo de control de acceso podemos obtener beneficios como los siguientes:

  - La identificación del personal biométrico no es transferible
  - Los costos de administración asociados y las tarjetas son eliminados
  - Opera individualmente o puede expandirse a un sistema multi-lectoras.

- Tarjetas de proximidad: La tecnología es llamada de proximidad porque la información de la tarjeta puede ser transmitida sin tocar la lectora.

- Sensores: Este dispositivo es el encargado de notificarnos el estado de la puerta. Cerrada o abierta

- Chapa: Este dispositivo eléctrico es el encargado de mantener cerrada o abierta nuestra puerta.

- Botón de Salida: Dispositivo mecánico que nos permite realizar la salida en el caso que sólo tenemos una lectora de entrada.

- PC y Software: Es la herramienta que nos sirve para programar el panel de Acceso y checar el estado del sistema. La PC no es necesaria estar en línea para que el equipo y el sistema siga operando. (TIA-942, 2018)

7.7 Vigilancia

Se debe de contar con un circuito cerrado de televisión o su acrónimo CCTV, (Closed Circuit Television), es una tecnología de vídeo vigilancia visual diseñada para supervisar una diversidad de ambientes y actividades. Se le denomina circuito cerrado ya que, al contrario de lo que pasa con la difusión, todos sus componentes están enlazados. Además, a diferencia de la televisión convencional, este es un sistema pensado para un número limitado de espectadores.

El circuito puede estar compuesto, simplemente, por una o más cámaras de vigilancia conectadas a uno o más monitores o televisores, que reproducen las imágenes capturadas por las cámaras. Aunque, para mejorar el sistema, se suelen conectar directamente o enlazar por red otros componentes como vídeos u ordenadores.

Se encuentran fijas en un lugar determinado. En un sistema moderno las cámaras que se utilizan pueden estar controladas remotamente desde una sala de control, donde se puede configurar su panorámica, enfoque, inclinación y zoom.
(TIA-942, 2018)

7.8 Barreras

Se debe de aplicar barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información “confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de datos así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos. Y sólo se permita acceder a ellos a las personas autorizadas para hacerlo. (TIA-942, 2018)

7.9 Iluminación

La TIA-942 (Telecomunicacion infraestruture Standard for data center) indica en la sección 5.3.5 –lighting que la iluminación mínima en un centro de datos, medida en el centro de los pasillos entre los gabinetes, a un metro de piso, debe ser de: 500lx(50 candelas) en el plano horizontal y 200lx (20 candelas) en el plano vertical. (TIA-942, 2018)

7.10 Guardias

Existen medidas de seguridad perimetral que buscan el resguardo ante accesos no autorizados de personas al centro de datos. Entre ellas podemos mencionar guardas de seguridad 24/7.

Todo esto debe de ser complementado con personal especializado que debe de estar permanentemente monitoreando lo que acontece con los sistemas para prevenir y detectar intrusiones y/o accesos indebidos.(TIA-942, 2018)

7.12 Plan de recuperación ante desastres.

De acuerdo a IBM de aquellas empresas que han tenido una pérdida de registro automatizados por un desastre, solo el 6% sobrevive a largo plazo, 51% cierra en menos de un año y 43% nunca vuelve abrir. (IBM, 2018)

Esta es la razón por la cual se debe de contar con un plan de recuperación ante desastres.

Las interrupciones del servicio, perdida de la información son factores que se ven impactados tras desastres.

Estos son factores a considerar:

- **Involucrar a todas las áreas:** Asignar responsabilidades y asegurar los recursos para la definición, planeación y ejecución en caso de contingencia.

- **Contemplar un análisis de impacto al negocio:** Definir cuál es la información del negocio que no puede perderse bajo ningún concepto o eventualidad.

- **Asignar prioridades del negocio:** Están se deben de definir con base al presupuesto que la empresa deberá destinar para el plan y elementos que se consideren críticos en la operación.

- **Tiempo máximo de recuperación:** se debe de tener un tiempo máximo tolerable en el que se pueda permanecer inactivo después de enfrentar un desastre.

- **Punto de recuperación:** Tiempo en el que los datos críticos se están respaldando (Frecuencia) Lo que tendrá igual impacto en el tiempo de restauración.

- **Pruebas de ejecución:** La única manera de garantizar que un plan de recuperación de desastre funcione en su totalidad será ejecutando simulacros en distintos escenarios con el alcance que se busca definir la verdadera efectividad.

- **Opciones de virtualización:** Existen muchas ventajas en la adopción de la virtualización en un plan de recuperación de desastres. Plataformas tecnológicas en la nube que periten adecuar los ambientes. (TIA-942, 2018)

Fase VIII: Evaluación de la Infraestructura, vías y espacios de cableado de telecomunicaciones

8.1 Introducción

El cableado a implementar en un centro de datos es de gran importancia porque este es el medio físico con el cual se conectan los diferentes dispositivos y es la forma como realmente se crea la arquitectura de la red. La transmisión de la información requiere cada vez más velocidad. Además, los equipos que se implementan y el tipo de cable han cambiado de cobre a fibra óptica. Este cambio continuo se da por la necesidad de los usuarios de aumentar la velocidad de conexión a los servicios que se ofrecen día a día. Es necesario que el centro de datos sea flexible; permitiendo así la mejora progresiva y la implementación de nuevos equipos y tipos de conexiones para que se cumpla con las necesidades de los usuarios.

8.2 Clases de infraestructura de cableado de telecomunicaciones

Las infraestructuras de cableado para diferentes tipos de aplicaciones, incluyendo edificios comerciales y residenciales. A grandes rasgos, existen tres tipos de estándares:

Los comunes, que establecen criterios genéricos, los que aplican según el tipo de local (Locales comerciales, residenciales, centros de datos, etc.) y los que detallan los componentes a utilizar, tanto en tecnología de “cobre” como de “fibra óptica”.

8.3 Topología de cableado

La norma EIA/TIA 568A hace las siguientes recomendaciones en cuanto a la topología.

Cada toma /conector de telecomunicaciones del área de trabajo debe de conectarse a una interconexión en el cuarto de telecomunicaciones.

La distancia horizontal no debe de exceder 90 m. la distancia se mide desde la interconexión en el cuarto de telecomunicaciones hasta el área de trabajo.

Además se recomienda las siguientes distancias: se separan 10 m para los cables de áreas de trabajo y los cables de cuarto de telecomunicaciones (cordones de parcheo, jumper y cables de equipo) (Norma EIA/TIA 568A , 2018)

8.4 Espacios de telecomunicaciones para el centro de datos

Es de fundamental importancia entender que para que un centro de datos quede exitosamente diseñado, construido y equipado para soportar los requerimientos actuales y futuros de los sistemas de telecomunicaciones, es necesario que el diseño de las telecomunicaciones

El estándar identifica seis componentes en la infraestructura edilicia:

- Instalaciones de Entrada
- Sala de Equipos
- Canalizaciones de “Montantes” (“Back-bone”)
- Salas de Telecomunicaciones
- Canalizaciones horizontales
- Áreas de trabajo

8.6 Cableado del eje central (backbone)

La función del “back-bone” es proveer interconexión entre los armarios de telecomunicaciones y las salas de equipos y entre las salas de equipos y las instalaciones de entrada.

Los sistemas de distribución central de cableado incluyen los siguientes componentes:

- Cables montantes
- Repartidores principales y secundarios
- Terminaciones mecánicas
- Cordones de interconexión o cables de cruzadas para realizar las
- conexiones entre distintos cables montantes.

El diseño de los sistemas de distribución central de cableado deben tener en cuenta las necesidades inmediatas y prever las posibles ampliaciones futuras, reservando lugar en el diseño de las canalizaciones, previendo cables con la cantidad adecuada de conductores, diseñando la cantidad de regletas o elementos de interconexión en los repartidores principales e intermedios, etc.

El estándar admite los siguientes cables para el Back-Bone:

- Cables UTP de 100 ohm (par trenzado sin malla)
- Cables de Fibra óptica multimodo de 50/125 µm
- Cables de Fibra ótpica multimodo de 62.5/125 µm
- Cables de Fibra ótpica monomodo
- Cable STP-A de 150 ohm (par trenzado con malla).(Norma EIA/TIA 568A , 2018)

8.7 Cableado horizontal

El cableado horizontal, ubicado en la Sala de Telecomunicaciones. Estos repartidores horizontales deben disponer de los elementos de interconexión adecuados para la terminación de los cables montantes (ya sean de cobre o fibra óptica).

Asimismo, a los repartidores horizontales llegan los cables provenientes de las “áreas de trabajo” (cableado horizontal, de allí su nombre de “repartidores horizontales”), el que también debe ser terminado en elementos de interconexión adecuado.

La función principal de los repartidores horizontales es la de interconectar los cables horizontales (provenientes de las áreas de trabajo) con los cables montantes (provenientes de la sala de equipos). Eventualmente, en la Sala de telecomunicaciones, puede haber equipos de telecomunicaciones, los que son incorporados al repartidor horizontal para su interconexión hacia la sala de equipos (a través del back-bone) y/o hacia las áreas de trabajo (a través del cableado horizontal).

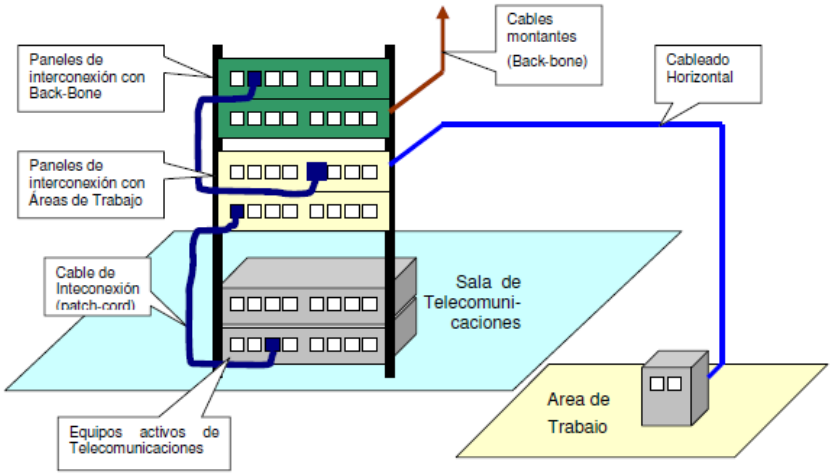


Figura 28: Cableado Horizontal

8.8 Instalación de cableado

El cableado dentro de un centro de datos se constituye en la arteria principal del flujo de información a través del mismo. Se debe garantizar no solo la conectividad TCP/IP, sino también que los dispositivos de red sean consistentes.

La mayor parte de estos requerimientos se puede cubrir utilizando cables categoría 5e, 6e o fibra óptica. Entender que equipos van y conocer los requisitos del cableado para cada parte del equipo se convierte en un factor indispensable al momento de construir un centro de datos.

8.9 Gabinetes y bastidores de telecomunicaciones y computadoras

Un gabinete para equipamiento completo requiere por lo menos 76,2 cm (30pulgadas) de espacio libre delante de la puerta para que ésta se pueda abrir. Los gabinetes para equipamiento tienen por lo general 1,8 m (5,9 pies) de alto, 0,74 m (2,4 pies) de ancho y 0,66 m (2.16 pies) de profundidad.

Cuando coloque el equipamiento dentro de los bastidores de equipos, tenga en cuenta si el equipo utiliza electricidad o no. Otras consideraciones a tener en cuenta son el tendido y administración de los cables y la facilidad de uso. Por ejemplo, un panel de conexión no debe colocarse en la parte de arriba de un bastidor si se van a realizar modificaciones significativas después de la instalación. Los equipos pesados como switches y servidores deben ser colocados cerca de la base del bastidor por razones de estabilidad.

La escalabilidad que permite el crecimiento futuro es otro aspecto a tener en cuenta en la configuración del equipamiento. La configuración inicial debe incluir espacio adicional en el bastidor para así poder agregar otros paneles de conexión o espacio adicional en el piso para instalar bastidores adicionales en el futuro. La instalación adecuada de bastidores de equipos y paneles de conexión permitirá, en el futuro, realizar fácilmente modificaciones a la instalación del cableado.

8.10 Administración de espacios, vías y cableado de telecomunicaciones

Los dispositivos de administración de cables son utilizados para tender cables a lo largo de un trayecto ordenado e impecable y para garantizar que se mantenga un radio mínimo de acodamiento. La administración de cables también simplifica el agregado de cables y las modificaciones al sistema de cableado.

Hay muchas opciones para la administración de cables dentro de la centro de datos. Los canastos de cables se pueden utilizar para instalaciones fáciles y livianas. Los bastidores en escalera se usan con frecuencia para sostener grandes cargas de grupos de cables. Se pueden utilizar distintos tipos de conductos para tender los cables dentro de las paredes, techos, pisos o para protegerlos de las condiciones externas. Los sistemas de administración de cables se utilizan de forma vertical y horizontal en bastidores de telecomunicaciones para distribuir los cables de forma impecable.(Norma EIA/TIA 568A , 2018)

Fase IX: Evaluación de las TI

9.1 Comunicaciones

Sin un ancho de banda y comunicaciones adecuadas el Centro de Datos pierde el valor. El tipo y calidad del ancho de banda depende de los dispositivos tantos activos como pasivos que se encuentren en el Centro de Datos, Un buen sistema de comunicaciones es la ruta principal para la conectividad entre los equipos y sus interconexiones.

9.2 Disposición de sala de computadoras

La salas de computadoras forman parte importante de un centro de datos ya que en ellas se llevan a cabo la labor de monitorear el buen funcionamiento de los servidores deben de estar disponibles las 24 horas 365 días al año con accesos a los colaboradores únicamente.

9.3 Centro de operaciones

Los centros de datos deben convertirse en motores de comunicación para irse adaptando y estar al día con las exigencias de aplicaciones emergentes de voz, datos, video y vigilancia.

Un centro de operaciones vincula todo esto:
Casi todos los sistemas de un edificio (HVAC, iluminación, vigilancia y comunicaciones) usan alguna forma de red TI para la administración y control.

Se debe de contar con monitoreo y control, de base IP, de los sistemas de edificios, a través de una infraestructura integrada e inteligente. Al combinar en una plataforma única operaciones segmentadas como la vigilancia, la red y las operaciones de manufactura, se pueden compartir datos entre aplicaciones, lo que

mejora la conciencia, la capacidad de respuesta y la eficacia operativas. (TIA-942, 2018)

9.4 Confiabilidad de la infraestructura de la red.

Las redes deben admitir una amplia variedad de aplicaciones y servicios, así como funcionar a través de los distintos tipos de cables y dispositivos que componen la infraestructura física. En este contexto, el término “arquitectura de red” se refiere a las tecnologías que dan soporte a la infraestructura y a los servicios y las reglas, o protocolos, programados que trasladan los datos a través de la red.

A medida que las redes evolucionan, descubrimos que existen cuatro características básicas que las arquitecturas subyacentes necesitan para cumplir con las expectativas de los usuarios. (TIA-942, 2018)

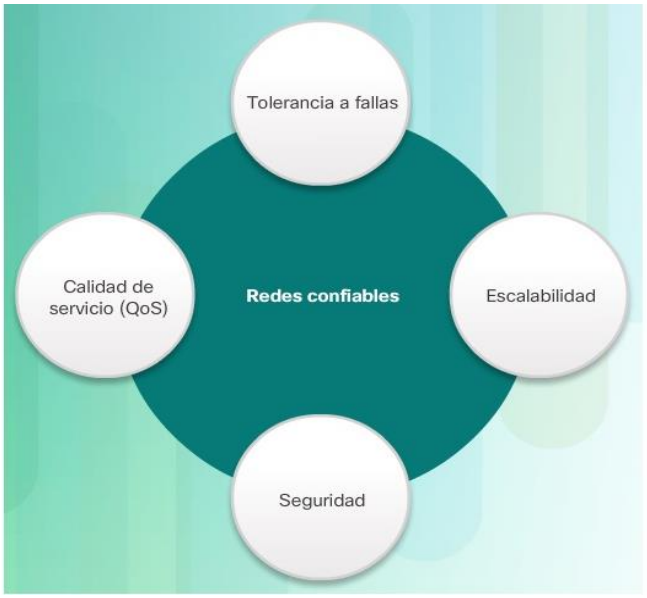


Figura 29: Diagrama de redes confiable

- **Tolerancia a fallas**

Una red con tolerancia a fallas es una que limita el impacto de las fallas, de modo que la cantidad de dispositivos afectados sea la menor posible, se arma de forma tal que permita una recuperación rápida cuando se produce una falla. Si falla una

ruta, los mensajes se pueden enviar inmediatamente por otro enlace. El hecho de que haya varias rutas que conducen a un destino se denomina “redundancia”.

Si una ruta utilizada anteriormente ya no está disponible, la función de enrutamiento puede elegir en forma dinámica la próxima ruta disponible. Debido a que los mensajes se envían por partes, en lugar de hacerlo como un único mensaje completo, los pocos paquetes que pueden perderse pueden volverse a transmitir al destino por una ruta diferente

- **Escalabilidad**

Una red escalable puede expandirse rápidamente para admitir nuevos usuarios y aplicaciones sin afectar el rendimiento del servicio enviado los usuarios actuales, también se refiere a la capacidad de admitir nuevos productos y aplicaciones.

- **Seguridad**

La infraestructura de red, los servicios y los datos contenidos en los dispositivos conectados a la red son activos comerciales y personales muy importantes. Si se pone en peligro la integridad de esos recursos, esto podría traer consecuencias graves, como las siguientes:

- Interrupciones de la red que impidan la comunicación y la realización de transacciones, lo que puede provocar pérdidas de negocios.
- Robo de propiedad intelectual (ideas de investigación, patentes y diseños) y uso por parte de la competencia.
- Información personal o privada que se pone en riesgo o se hace pública sin el consentimiento de los usuarios.
- Mala orientación y pérdida de recursos personales y comerciales.

- Pérdida de datos importantes cuyo reemplazo requiere un gran trabajo o que son irreemplazables.

La seguridad de una infraestructura de red incluye el aseguramiento físico de los dispositivos que proporcionan conectividad de red y prevenir el acceso no autorizado al software de administración que reside en ellos.

Para alcanzar los objetivos de seguridad de red, hay tres requisitos principales:

- **Asegurar la confidencialidad:** la confidencialidad de los datos se refiere a que solamente los destinatarios deseados y autorizados (personas, procesos o dispositivos) pueden acceder a los datos y leerlos (La encriptación de datos).
- **Mantener la integridad de la comunicación:** la integridad de los datos se relaciona con tener la seguridad de que la información no se alteró durante la transmisión desde el origen hasta el destino. La integridad de los datos se puede poner en riesgo si se daña la información, ya sea voluntaria o accidentalmente. Se puede asegurar la integridad de los datos mediante la solicitud de validación del emisor así como promedio del uso de mecanismos para validar que el paquete no se modificó durante la transmisión.

- **Asegurar la disponibilidad:** la disponibilidad se relaciona con tener la seguridad de que los usuarios autorizados contarán con acceso a los servicios de datos en forma confiable y oportuna. Los dispositivos de firewall de red, junto con el software antivirus de los equipos de escritorio y de los servidores pueden asegurar la confiabilidad y la solidez del sistema para detectar, repeler y resolver esos ataques. Real infraestructuras de red totalmente redundantes, con pocos puntos de error únicos, puede reducir el impacto de estas amenazas. (TIA-942, 2018)

- **QoS, Quality of Service**

Las redes deben proporcionar servicios predecibles, mensurables y, en ocasiones, garantizados. Cuando se producen intentos de comunicaciones simultáneas a través de la red, la demanda de ancho de banda puede exceder su disponibilidad, lo que provoca congestionen la red. El secreto para ofrecer una solución de calidad de aplicación de extremo a extremo exitosa es lograr la QoS necesaria mediante la administración de los parámetros de retraso y de pérdida de paquetes en una red. Una de las formas en que esto se puede lograr es mediante la clasificación. Para crear clasificaciones de QoS de datos, utilizamos una combinación de características de comunicación y la importancia relativa que se asigna a la aplicación. Algunas de las decisiones prioritarias para una organización pueden ser:

- **Comunicaciones dependientes del factor tiempo:** aumento de la prioridad para servicios como la telefonía o la distribución de videos.

- **Comunicaciones independientes del factor tiempo:** disminución de la prioridad para la recuperación de páginas Web o correos electrónicos.

- **Suma importancia a la organización:** aumento de la prioridad de los datos de control de producción o transacciones comerciales.

- **Comunicaciones no deseadas:** disminución de la prioridad o bloqueo de la actividad no deseada, como intercambio de archivos punto a punto o entretenimiento en vivo.

9.5 Seguridad para redes de TI y de instalaciones

En esta parte del plan se incluye las acciones se incluye las acciones a realizar para garantizar la seguridad de las redes y sus servicios, mediante la habilitación de las opciones de seguridad con que cuentan con los sistemas operativos y de otras iniciativas dirigidas a lograr la seguridad de los servidores y terminales, el acceso a

la información solamente al personal autorizado y los elementos que permitan el monitoreo y la auditoria de los principales elementos:

- Barreas de protección y su arquitectura
- Empleo de cortafuego, sistemas proxy etc.
- Filtrado de paquetes.
- Herramientas de administración y monitoreo.
- Establecimiento de alarmas del sistema.
- Dispositivos de identificación y autentificación de usuarios
- Software especial de seguridad.
- Medios técnicos y detección de intrusos. (IPS/IDS).

Se deben de especificar los procedimientos requeridos para el cumplimiento de las obligaciones de los administradores de redes con relación a la seguridad en particular a los relacionados con:

La aplicación de mecanismos que implementan las políticas de seguridad aprobada. El análisis sistemático de los registros de la auditoria que proporciona el sistema operativo de la red.

Las acciones de respuesta en caso de la ocurrencia de actividades o acciones nocivas.

Se incluirá los procedimientos instrumentados para la verificación de la seguridad de las redes y a detección de las vulnerabilidades. (TIA-942, 2018)

Fase X: Evaluación de la infraestructura usando Tiers

Guía de referencia de niveles (telecomunicaciones)

Telecomunicaciones	Tier 1	Tier 2	Recomendaciones
Cableado, bastidores, gabinetes y vías que cumplen con especificaciones TIA relevantes.	SI	SI	
Entradas de proveedores de acceso diversamente enrutadas y Agujeros de mantenimiento con un mínimo de 20 m	No requerido	SI	
Servicios de proveedor de acceso redundante: múltiples proveedores de acceso, oficinas centrales, proveedor de acceso derecho de paso	No requerido	No requerido	
Sala de entrada redundante	No requerido	No requerido	
Área de distribución principal redundante	No requerido	No requerido	
Áreas de distribución intermedias redundantes (si están presentes)	No requerido	No requerido	
Redondeo de cableado y vías principales	No requerido	No requerido	
Cableado horizontal redundante y vías	No requerido	No requerido	
Los enrutadores y conmutadores tienen fuentes de alimentación redundantes, procesadores	No requerido	SI	
Enrutadores e interruptores redundantes con redundancia enlaces ascendentes	No requerido	No requerido	
Paneles de conexión, tomacorrientes y cableado que se etiquetarán por ANSI / TIA-606-B. Armarios y estanterías para etiquetar delantero y trasero.	SI	SI	
Cables de conexión y puentes para etiquetar en ambos extremos con el nombre de la conexión cable	No requerido	SI	
Documentación del panel de parche y del cable de parche con ANSI / TIA-606-B	No requerido	No requerido	

Guía de referencia de niveles (arquitectónica)

ARQUITECTURA	Tier 1	Tier 2	Recomendaciones
Proximidad al área de peligro de inundación según se mapea en un Límite federal de riesgo de inundación o seguro contra inundaciones Mapa de tarifas	No requerido	No dentro del riesgo de inundación de 50 años área	
Proximidad a las vías navegables costeras o navegables	No requerido	No requerido	
La proximidad a las principales arterias de tráfico de carretera y principal líneas de ferrocarril	No requerido	No requerido	
Proximidad a las tarifas	No requerido	No requerido	
Parking			
Estacionamiento separado para visitantes y empleados	No requerido	No requerido	
Separado de los muelles de carga	No requerido	No requerido	
Proximidad del estacionamiento de visitantes al perímetro del centro de datos construyendo muros	No requerido	No requerido	
Ocupación de varios inquilinos dentro del edificio	Sin restricción	Permitido solo si las ocupaciones no son peligrosas	
Construcción de edificios			
Tipo de construcción (IBC 2006)	Sin restricción	Sin restricción	
Requisitos de resistencia al fuego			
Muros de carga exterior	Código permitido	Código permitido	
Muros de carga interiores	Código permitido	Código permitido	
Muros exteriores no portantes	Código permitido	Código permitido	

Marco estructural	Código permitido	Código permitido	
Muros divisorios interiores para salas que no son para computadora	Código permitido	Código permitido	
Paredes interiores de la sala de ordenadores Shalth	Código permitido	Código permitido	
Pisos	Código permitido	Código permitido	
Techos	Código permitido	Código permitido	
Cumplir con los requisitos de NFPA 75	Código permitido	Código permitido	

Componentes diversos de construcción	**Tier 1**	**Tier 2**	**Recomendaciones**
Barreras de vapor para paredes y techo de computadora habitación	Sin restricción	sí para las paredes, no requerido para techo	
Entradas de edificios con puntos de control de seguridad	Sin requisito	Sin requisito	
Infraestructura (cuando se proporciona el piso de acceso)	Sin requisito	Sin requisito	
Techado			
Clase	Sin requisito	Clase A	
Tipo	Sin requisito	Sin requisito	
Resistencia al levantamiento del viento	Requisitos mínimos del código	FM I-90	
Pendiente del Techo	Requisitos Mínimo de código	Requisitos mínimos de código	
Puertas y ventanas			
Clasificación de fuego	Requisitos mínimos de código	Requisitos mínimos de código	

Tamaño de la puerta	Requisitos mínimos de código y no menos de 1 m (3 pies) de ancho y 2,13 m (7 pies) de alto	Requisitos mínimos de código y no menos de 1 m (3 pies) de ancho y 2,13 m (7 pies) de alto	
Windows en el perímetro de la sala de ordenadores	Permitido con un código mínimo calificación de fuego requerida	Permitido con un código mínimo calificación de fuego requerida	
Vestíbulo de entrada	Físicamente separado de otras áreas del centro de datos	SI	
Incendio desde otras áreas del centro de datos	Requisitos mínimos del código		
Contador de seguridad	No requerido	No requerido	
Enclavamiento de persona única, portal u otro hardware diseñado para evitar el transporte a cuestas o el regreso	No requerido	No requerido	

Oficinas Administrativas	**TIER 1**	**Tier 2**	**Recomendaciones**
Físicamente separado de otras áreas del centro de datos	No requerido	SI	
Incendio desde otras áreas del centro de datos	Requisitos mínimos del código	Requisitos mínimos del código	
Oficina de seguridad			
Físicamente separado de otras áreas del centro de datos	No requerido	No requerido	
Incendio desde otras áreas del centro de datos	Requisitos mínimos del código	Requisitos mínimos del código	

Mirillas de 180 grados en equipos de seguridad y salas de monitoreo	No requerido	SI	
Equipo de seguridad dedicado y reforzado salas de monitoreo	No requerido	SI	
Centro de operaciones			
Centro de operaciones físicamente separado de otros áreas del centro de datos	No requerido	No requerido	
Incendio desde otra habitación que no sea computadora áreas del centro de datos	No requerido	No requerido	
Proximidad a la sala de ordenadores	No requerido	No requerido	
Baños y salas de descanso			
Proximidad a la sala de computadoras y áreas de apoyo	No requerido	No requerido	
Separación de fuego de la sala de ordenadores y soporte áreas	No requerido	Requisitos mínimos de código	
Ups y baterías			
Anchos de pasillo para mantenimiento, reparación o equipamiento eliminación	No requerido	No requerido	
Proximidad a la sala de ordenadores	No requerido	No requerido	
Separación de fuego de la sala de computadoras y otros áreas del centro de datos	Requisitos mínimo del código	Requisitos mínimo del código	
Corredores de salida obligatorios			
Separación de fuego de la sala de ordenadores y soporte áreas	Requisitos mínimo del código	Requisitos mínimo del código	
Ancho	Requisitos mínimo del código	Requisitos mínimo del código	

Área de envío y recepción	**Tier 1**	**Tier 2**	**Recomendaciones**
Área de envío y recepción separada físicamente desde otras áreas del centro de datos	Sin área de envío y recepción proporcionado	No requerido	
Incendio desde otras áreas del centro de datos	Requisitos mínimos del código si área de envío y servicio presente	Requisitos mínimos del código	
Protección física de las paredes tráfico de equipo	No requerido	No requerido	
Número de muelles de carga	No requerido	1 por 2500 m (25,000 pies)) de Sala de ordenadores	
Áreas de almacenamiento de generador y combustible			
Proximidad a la sala de computadoras y áreas de apoyo	No requerido	No requerido	
Proximidad a las áreas de acceso público	No requerido	No requerido	
Seguridad			
Capacidad del UPS de la CPU del sistema	No requerido	Edificio	
Paneles de recopilación de datos (paneles de campo) Capacidad de UPS	No requerido	Edificio + batería (4 horas min)	
Capacidad UPS del dispositivo de campo	No requerido	Edificio + batería (4 horas min)	
Personal de seguridad	No requerido	Durante la operación programada (típicamente 5 días a la semana para normal horario comercial)	

Control de acceso / monitoreo de seguridad en	**Tier 1**	**Tier 2**	**Recomendaciones**
Generadores	cerradura de grado industrial	Detección de intrusos	
UPS, teléfono y habitaciones MEP	cerradura de grado industrial	Detección de intrusos	
Bóvedas de fibra	cerradura de grado industrial	Detección de intrusos	
Puertas de salida de emergencia	cerradura de grado industrial	Monitor	
Ventanas / aberturas exteriores accesibles	No requerido	Detección de intrusos (con fuera de sitio monitoreo durante los turnos cuando no personal de seguridad está presente)	
Centro de operaciones de seguridad	No requerido	No requerido	
Centro de operaciones de red	No requerido	No requerido	
Salas de equipos de seguridad	No requerido	Detección de intrusos	
Puertas en salas de computadoras	cerradura de grado industrial	Detección de intrusos	
Puertas de construcción perimetrales	No requerido	detección de intrusos (con fuera de sitio monitoreo durante los turnos cuando no personal de seguridad está presente)	
Puerta principal en el piso de la sala de computadoras	cerradura de grado industrial	Acceso a la tarjeta	
Paredes, ventanas y puertas resistentes a balas			
Mostrador de seguridad en el lobby	No requerido	No requerido	
Monitoreo CCTV			
Construcción de perímetro y estacionamiento	No requerido	No requerido	

Generadores	No requerido	No requerido	
Acceso a puertas controladas	No requerido	SI	
Pisos de la habitación de la computadora	No requerido	No	
UPS, teléfono y habitaciones MEP	No requerido	No requerido	
CCTV			
CCTV Grabación de toda la actividad en todas las cámaras	No requerido	No requerido	
Velocidad de grabación (cuadros por segundo)	No requerido	No requerido	

Estructural	**Tier 1**	**Tier 2**	**Recomendaciones**
Diseño de instalaciones para el Código Internacional de Construcción (IBC) Requisitos de la Categoría de diseño sísmico (SDC)	Use los requisitos de SDC para construir ubicación	use los requisitos de SDC para construir ubicación	
Espectro de respuesta específica del sitio Grado de local Aceleraciones sísmicas	No requerido	No requerido	
factor de importancia ayuda a garantizar mayor que diseño de código	I=1	I=1.5	
Bastidores / armarios para equipos de telecomunicaciones anclado a la base	No requerido	Solo base	
Limitación de deflexión en telecomunicaciones equipo dentro de aceptable archivos adjuntos	No requerido	No requerido	
Arrostramiento de conductos eléctricos y bandejas de cables	por código	por código w / importancia	
Arrostramiento del sistema mecánico	por código	por código w / importancia	

Capacidad de carga del piso superpuesta carga viva	7.2 kPa (150lbf/ft).	8.4 kPa (175 lbf/ft)	
Capacidad de colgar en el piso para cargas auxiliares suspendidas desde abajo	2 kPa (25 lbf/ft)	1.2 kPa (25 lbf/ft)	
Grueso de la losa de hormigón en el suelo	127 mm (5 in)	127 mm (5 in)	
Revestimiento mínimo de hormigón sobre flautas para equipos anclaje utilizado para pisos elevados	102 mm (4 in)	102 mm (4 in)	
Construcción de LFRS (Shearwall / Braced Frame / Moment Marco) indica el desplazamiento de la estructura	Marco de momento de acero / hormigón	Shearwall de hormigón / acero reforzado Marco	
Disipación de energía del edificio - Amortiguadores pasivos / Base Aislamiento (absorción de energía)	No requerido	No requerido	
Construcción de piso elevado. (Estructuras de acero con las cubiertas de metal rellenas de hormigón se actualizan más fácilmente para cargas extremas en salas de batería / UPS. (Además, mejor para instalar anclajes de piso).	Hormigón PT	Hormigón suave	

ELECTRICO	Tier 1	Tier 2	Recomendaciones
El sistema permite el mantenimiento concurrente	No requerido	Utilidad, generador y sistema UPS	
Punto único de falla	Múltiples puntos únicos de falla a lo largo de la distribución sistema	Múltiples puntos únicos de falla en todo el sistema de distribución	
Análisis del sistema de potencia	Estudio actualizado de cortocircuitos estudio de coordinación, y análisis de arco de flash	Estudio actualizado de cortocircuitos estudio de coordinación, y análisis de arco de flash	
Equipo de Computación y Telecomunicaciones Cables de alimentación	Alimentación de cable único con 100% capacidad	Alimentación de cable único con 100% capacidad	
Utilidad			
Entrada de servicios públicos	Una alimentación	Una alimentación	
Cuadro de distribución de la utilidad principal			
Servicio	Compartido	Compartido	
Construcción	Tablero con circuito atornillado interruptores	Panel de control con circuito todo en uno interruptores	
Supresión de sobretensiones	No requerido	No requerido	

Sistema de alimentación ininterrumpida	**Tier 1**	**Tier 2**	**Recomendaciones**
Redundancia	N	N	
Topología	Módulos individuales o paralelos	Módulos individuales o paralelos	
Derivación automático	No requerido	Sí, sin un alimentador dedicado a derivación automática	
Arreglo de desvío de mantenimiento	No requerido	Mantenimiento no dedicado derivación del alimentador a la salida del UPS centralita	
Distribución de potencia de salida	Tablero que incorpora viaje magnético térmico estándar interruptores	Tablero que incorpora viaje magnético térmico estándar interruptores	
Cadena de batería	Cadena común para múltiples módulos	Cadena dedicado para cada módulo	
Tipo de batería	Ácido de plomo regulado por válvula de 5 años o volante	Válvula de 10 años o tipo inundado o volante	
Tiempo de respaldo mínimo de la batería con carga de diseño en fin de la duración de la batería	5 Minutos	6 Minutos	
Sistema de monitoreo de la batería **Unidad de distribución de energía**	No requerido	No requerido	
Transformador	Alta eficiencia estándar	Alta eficiencia estándar	
Interruptor de transferencia estático automático	No requerido	No requerido	
Dispositivo de sobre corriente	No requerido	No requerido	

Procedimiento de derivación de mantenimiento	No requerido	No requerido	
Salida	No requerido	No requerido	

Conexión a tierra	**Tier 1**	**Tier 2**	**Recomendaciones**
Sistema de protección contra rayos	Basado en el análisis de riesgo según NFPA 780 y seguro requisitos	Basado en el análisis de riesgo según NFPA 780 y seguro requisitos.	
Accesorios de iluminación neutralizados del servicio entrada derivada del transformador de iluminación para aislamiento de falla a tierra	No requerido	No requerido	
Infraestructura de conexión a tierra del centro de datos en la computadora habitación	Según lo requerido por ANSI / TIA-607-B	Según lo requerido por ANSI / TIA-607-B	
Apagado de emergencia de la sala de ordenadores (EPO) Sistema			
Instalación	Si AHJ lo requiere, presione para activar con protector de cubierta y etiqueta de advertencia	Si AHJ lo requiere, presione para activar con protector de cubierta y etiqueta de advertencia	
Modo de prueba	No requerido	No requerido	
Alarma	No requerido	No requerido	
Interruptor de cancelación	No requerido	No requerido	
Monitoreo de energía central			

Puntos monitoreados	No requerido	Utilidad UPS Generador	
Método de notificación	No requerido	Consola de la sala de control	
Habitación de batería			
Separado de las salas de equipos UPS / Switchgear	No requerido	No requerido	
Cadenas de batería individuales aisladas entre sí	No requerido	No requerido	
Vidrio de visualización inastillable en la puerta de la habitación de la batería	No requerido	No requerido	

Sistema generador en espera	**Tier 1**	**Tier 2**	**Recomendaciones**
Tamaño del generador	Tamaño solo para UPS sistemas sin redundancia	Tamaño para UPS y mecánico sistema sin redundancia	
Generadores en un solo bus	SI	SI	
Banco de carga			
Instalación	No requerido	provisión para portable	
Equipo probado	No requerido	Generador	
Apagado automático	No requerido	No requerido	
Prueba			
Prueba de aceptación de fábrica	No requerido	No requerido	
Prueba del interruptor de circuito del sitio	No requerido	No requerido	
Comisionamiento	No requerido	Nivel de componente	
Mantenimiento del equipo			
Personal de Operación y Mantenimiento	Fuera del sitio. En llamada.	Cambio de día en el sitio solamente. De guardia en otras veces	

Mantenimiento Preventivo	No requerido	Mantenimiento del generador	
Programas de capacitación de instalaciones	No requerido	Entrenamiento limitado por el fabricante	

MECÁNICO	**Tier 1**	**Tier 2**	**Recomendaciones**
Redundancia para equipos mecánicos (por ejemplo, aire unidades de acondicionamiento, enfriadores, bombas, torres de enfriamiento, condensadores)	No requerido	N + 1 redundancia para mecánica equipo. Pérdida de electricidad pérdida de potencia	
El enrutamiento de las tuberías de agua o drenaje no está asociado con centro de datos	Permitido pero no recomendado	Permitido pero no recomendado	
Presión positiva en la sala de informática y asociados espacios relativos al exterior y al centro no de datos espacios	No requerido	SI	
Desagües de piso en la sala de computadoras para el drenaje de condensados agua, humidificador, agua de lavado y rociadores descargar agua	SI	SI	
Sistemas mecánicos en el generador de reserva	No requerido	SI	
Sistema enfriado por agua			
Unidades de aire acondicionado de la terminal interior	Sin aire acondicionado redundante unidades	Una unidad de CA redundante por crítico área	
Control de humedad para la sala de ordenadores	No requerido	Humidificación proporcionada	
Servicio eléctrico para equipo mecánico	Una sola ruta de energía eléctrica para Equipo AC	Una sola ruta de energía eléctrica para Equipo AC	

Rechazo de calor			
Sistema de tuberías	Agua de condensador de una sola trayectoria sistema	Agua de condensador de una sola trayectoria sistema	
Sistema de tubería de agua enfriada	Sistema de agua fría de una sola vía	Sistema de agua fría de una sola vía	
Sistema de tubería de agua de condensador	Agua de condensador de una sola trayectoria sistema	Agua de condensador de una sola trayectoria sistema	

Sistema de agua enfriada	**Tier 1**	**Tier 2**	**Recomendaciones**
Control de humedad para la sala de ordenadores	No requerido	Humidificación proporcionada	
Servicio eléctrico para equipo mecánico	Una sola ruta de energía eléctrica para Equipo AC	Una sola ruta de energía eléctrica para Equipo AC	
Sistema enfriado por aire			
Servicio eléctrico para equipo mecánico	Una sola ruta de energía eléctrica para Equipo AC	Una sola ruta de energía eléctrica para Equipo AC	
Control de humedad para la sala de ordenadores	No requerido	Humidificación proporcionada	
Sistema de control HVAC			
Sistema de control HVAC	Fallo del sistema de control interrumpir el enfriamiento a áreas críticas	La falla del sistema de control no interrumpir el enfriamiento a áreas críticas	
Plomería (para rechazo de calor refrigerado por agua)			

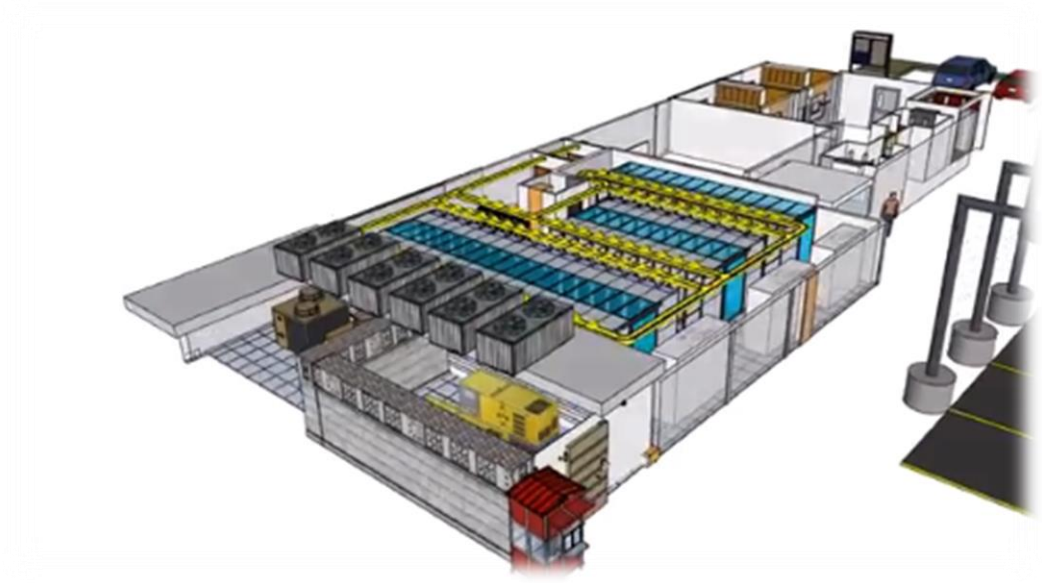
Agua de maquillaje	Suministro de agua individual, sin encendido almacenamiento de respaldo del sitio	Dos fuentes de agua, o una fuente + almacenamiento en el sitio	
Puntos de conexión al sistema de agua del condensador	Único punto de conexión	Único punto de conexión	
Sistema de aceite			
Tanques de almacenamiento a granel	Tanque de almacenamiento individual	Tanques de almacenamiento individual	
Bombas y tuberías de tanques de almacenamiento	Bomba única y / o tubería de suministro	Múltiples bombas, suministro múltiple tubos	
Supresión de fuego			
Sistema de detección de fuego	SI	SI	
Sistema de riego contra incendios	Cuando sea necesario	Acción previa (cuando sea necesario)	
Sistema de supresión gaseosa	Ningún requisito arriba AHJ	Ningún requisito arriba AHJ	
Sistema de detección de humo de alerta temprana	Ningún requisito arriba AHJ	SI	
Sistema de detección de fugas de agua	Ningún requisito arriba AHJ	SI	

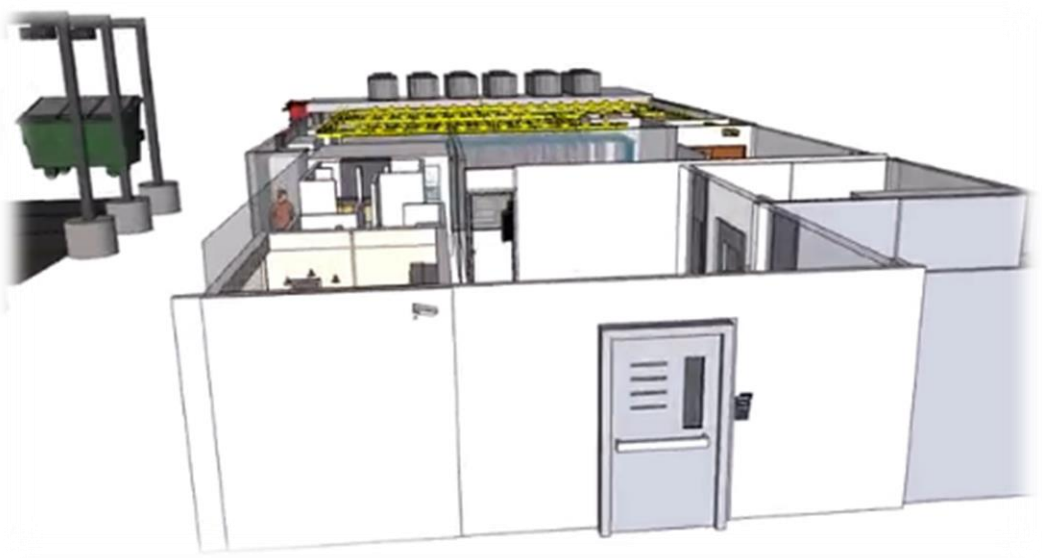
Beneficios de obtener una certificación

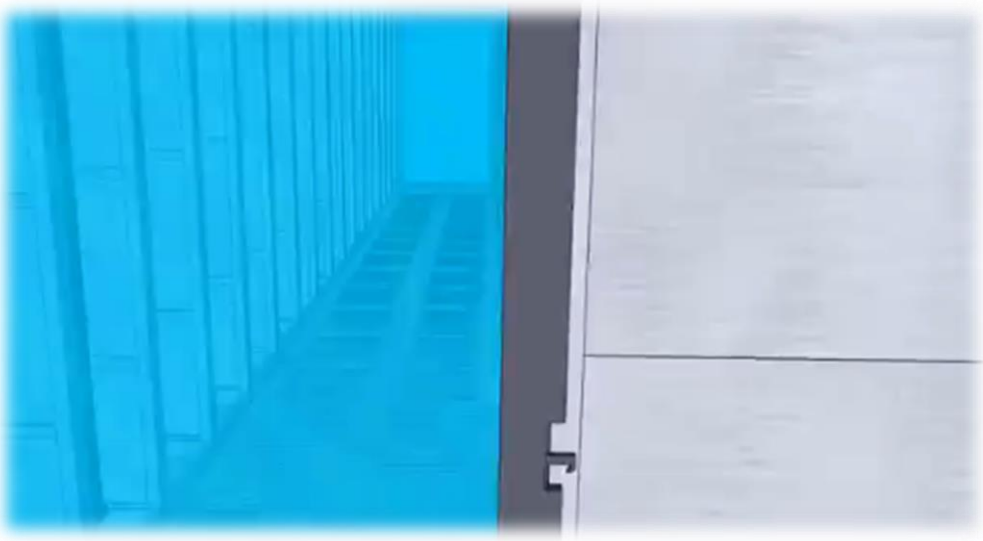
- Obtener las mejores prácticas y alcanzar todo el potencial de la infraestructura instalada.
- Identificación de los problemas de operaciones y administración que pueden comprometer la confiabilidad y el desempeño.
- Contar con un centro de datos menos susceptible a operaciones.
- Escalabilidad, que permite la posibilidad de ampliar o reducir los recursos contratados por las empresas.
- flexibilidad en modificaciones de servicios.
- Personal especializado y atención las 24 horas al día los 365 días del año.

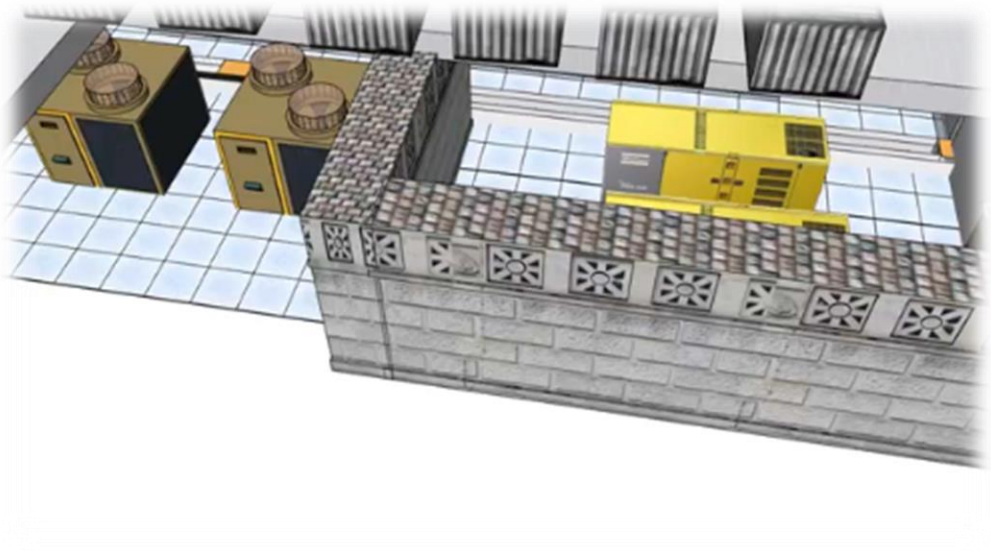
Prototipo de centro de datos con certificación TIER ll

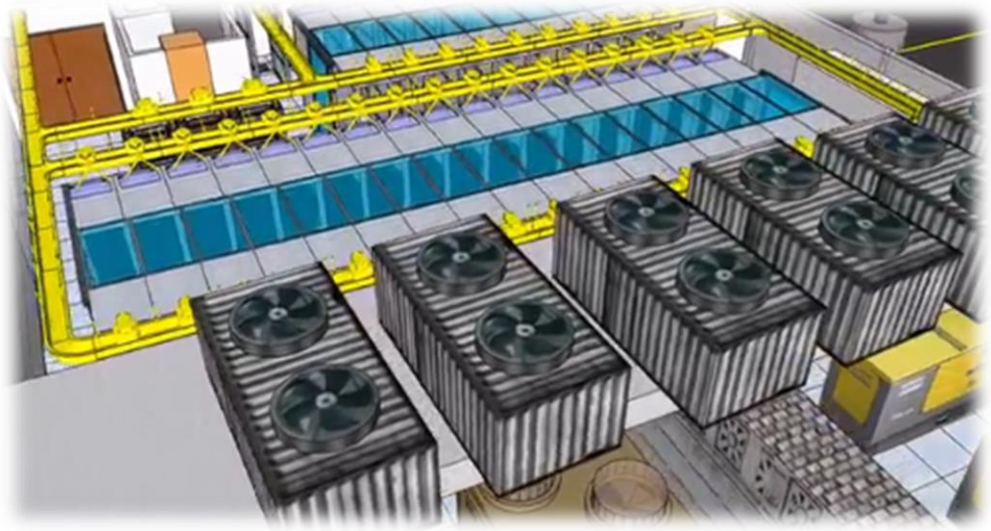
Se elaboró un prototipo de centro de datos con certificación TIER ll siguiendo las recomendaciones la norma TIA-942, se muestran en las siguientes imágenes:

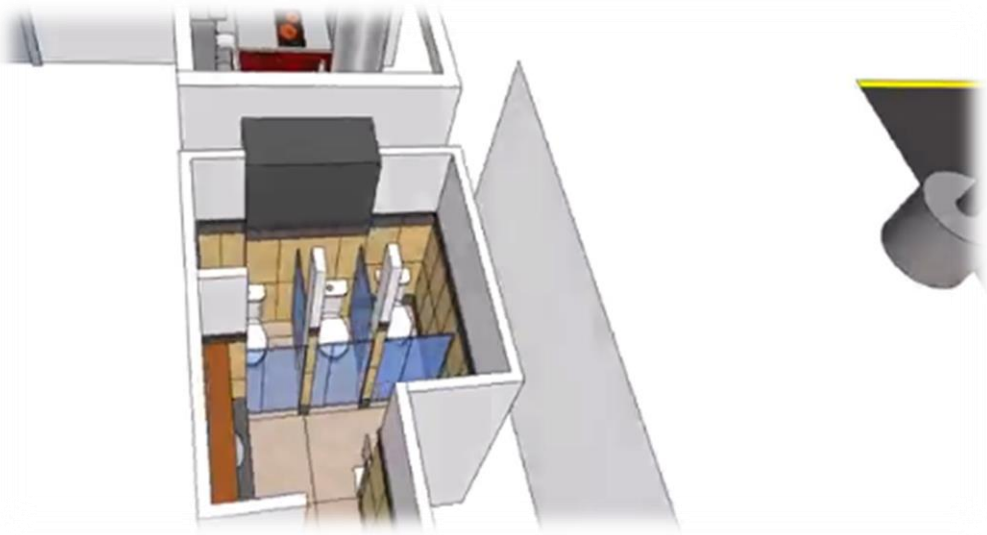












RECOMENDACIONES

- Se recomienda realizar mantenimiento al piso Falso.
- Etiquetar los cables en ambos extremos según lo establecido por la norma TIA-942.
- Se recomienda realizar revisión de los rack y bastidores instalados en el centro de datos.
- Realizar reparación de la energía de respaldo (Planta Eléctrica).
- Reforzar la seguridad perimetral del centro de Datos.
- Se recomienda construir un lugar especializado para el consumo de alimentos y que los administradores no ingresen con alimentos a la sala de monitoreo.
- Se recomienda que el sistema de climatización maneje los parámetros de temperatura y humedad dentro del centro de datos entre 17 °C y 25 °C.

CONCLUSIONES

- Se elaboró una propuesta de certificación TIER ll que permita evaluar los niveles de cumplimiento de la norma TIA-942 en el Centro Nacional de Datos Fiscales de la Dirección General de Ingresos (DGI).

- Se analizó la importancia y los beneficios de implementar la norma TIA-942 para la certificación TIER ll.

- Se evaluaron los niveles de cumplimiento del centro de datos de la dirección general de ingresos con respecto a la norma TIA-942 mediante una encuesta realizada a la unidad de base de Datos y sistemas operativos.

- Se realizó un prototipo de centro de centro de datos con certificación TIER ll siguiendo las recomendaciones establecida por la norma Tia-942.

ANEXOS

Anexo A: Encuesta realizada al área de unidad de bases de datos y sistemas operativos que está a cargo del centro de datos de la Dirección general de ingresos

Propuesta para la certificación TIER II del Centro de Datos de la Dirección General de Ingresos.

Encuestado/a: Isayana Banilla Montano Fecha: 05 / 10 / 2018

Cargo: Jefe de Unidad de Bases de Datos y S.O.

1. ¿El centro de datos se ubica en un área con peligro de inundación?

☐ SI ☑ NO

☐ Otra (por favor, especifique)

2. ¿Los Gabinetes y Racks están rotulados en la parte frontal y trasera?

☐ SI ☐ NO

☑ Otra (por favor, especifique) Solamente en la parte frontal

3. ¿El centro de datos posee UPS?

☑ SI ☐ NO

☐ Otra (por favor, especifique)

4. ¿El Generador está correctamente dimensionado de acuerdo a las capacidades de las UPS instaladas?

☑ SI ☐ NO

☐ Otra (por favor, especifique)

5. Supresión de Fuego: ¿Existe sistema de rociadores proactivo? (cuando se requieran)

☑ SI ☐ NO

Propuesta para la certificación TIER II del Centro de Datos de la Dirección General de Ingresos.

☐ Otra (por favor, especifique)

6. ¿El centro de datos posee piso elevado?

☑ SI ☐ NO

☐ Otra (por favor, especifique)

7. ¿El centro de datos cuenta con Lobby de entrada?

☑ SI ☐ NO

☐ Otra (por favor, especifique)

8. ¿Posee Control acceso de seguridad y monitoreo en puertas de salas de computadores con detección de intrusos?

☑ SI ☐ NO

☐ Otra (por favor, especifique)

9. ¿Existe Control de Humedad para sala de computadores a través de Humidificación?

☑ SI ☐ NO

☐ Otra (por favor, especifique)

10. ¿Existen PDUS de alimentación en todos los equipos de telecomunicaciones y computadores?

☑ SI ☐ NO

☐ Otra (por favor, especifique)

Propuesta para la certificación TIER II del Centro de Datos de la Dirección General de Ingresos.

Encuestado/a: Fernando Delgado Fecha: 05/10/2018

Cargo: Líder de DC

1. ¿El centro de datos se ubica en un área con peligro de inundación?

☐ SI ☒ NO

☐ Otra (por favor, especifique)

2. ¿Los Gabinetes y Racks están rotulados en la parte frontal y trasera?

☒ SI ☐ NO

☐ Otra (por favor, especifique)

3. ¿El centro de datos posee UPS?

☒ SI ☐ NO

☐ Otra (por favor, especifique)

4. ¿El Generador está correctamente dimensionado de acuerdo a las capacidades de las UPS instaladas?

☒ SI ☐ NO

☐ Otra (por favor, especifique)

5. Supresión de Fuego: ¿Existe sistema de rociadores proactivo? (cuando se requieran)

☒ SI ☐ NO

Propuesta para la certificación TIER II del Centro de Datos de la Dirección General de Ingresos.

☐ Otra (por favor, especifique)

6. ¿El centro de datos posee piso elevado?

☒ SI ☐ NO

☐ Otra (por favor, especifique)

7. ¿El centro de datos cuenta con Lobby de entrada?

☒ SI ☐ NO

☐ Otra (por favor, especifique)

8. ¿Posee Control acceso de seguridad y monitoreo en puertas de salas de computadores con detección de intrusos?

☒ SI ☐ NO

☐ Otra (por favor, especifique)

9. ¿Existe Control de Humedad para sala de computadores a través de Humidificación?

☐ SI ☒ NO

☐ Otra (por favor, especifique)

10. ¿Existen PDUS de alimentación en todos los equipos de telecomunicaciones y computadores?

☒ SI ☐ NO

☐ Otra (por favor, especifique)

Propuesta para la certificación TIER II del Centro de Datos de la Dirección General de Ingresos.

Encuestado/a: Nestor William Pineda Mejía Fecha: 05/10/2018

Cargo: Administrador De Bases de Datos.

1. ¿El centro de datos se ubica en un área con peligro de inundación?

☐ SI ☑ NO

☐ Otra (por favor, especifique)

2. ¿Los Gabinetes y Racks están rotulados en la parte frontal y trasera?

☐ SI ☑ NO

☐ Otra (por favor, especifique)

3. ¿El centro de datos posee UPS?

☑ SI ☐ NO

☐ Otra (por favor, especifique)

4. ¿El Generador está correctamente dimensionado de acuerdo a las capacidades de las UPS instaladas?

☑ SI ☐ NO

☐ Otra (por favor, especifique)

5. Supresión de Fuego: ¿Existe sistema de rociadores proactivo? (cuando se requieran)

☑ SI ☐ NO

Propuesta para la certificación TIER II del Centro de Datos de la Dirección General de Ingresos.

☐ Otra (por favor, especifique)

6. ¿El centro de datos posee piso elevado?

☑ SI ☐ NO

☐ Otra (por favor, especifique)

7. ¿El centro de datos cuenta con Lobby de entrada?

☑ SI ☐ NO

☐ Otra (por favor, especifique)

8. ¿Posee Control acceso de seguridad y monitoreo en puertas de salas de computadores con detección de intrusos?

☑ SI ☐ NO

☐ Otra (por favor, especifique)

9. ¿Existe Control de Humedad para sala de computadores a través de Humidificación?

☑ SI ☐ NO

☐ Otra (por favor, especifique)

10. ¿Existen PDUS de alimentación en todos los equipos de telecomunicaciones y computadores?

☑ SI ☐ NO

☐ Otra (por favor, especifique)

Propuesta para la certificación TIER II del Centro de Datos de la Dirección General de Ingresos.

Encuestado/a: José A. Herrera Fecha: 05/10/2018

Cargo: Jefe oficina Apoyo tecnologico

1. ¿El centro de datos se ubica en un área con peligro de inundación?

☐ SI ☒ NO

☐ Otra (por favor, especifique)

2. ¿Los Gabinetes y Racks están rotulados en la parte frontal y trasera?

☐ SI ☒ NO

☐ Otra (por favor, especifique)

3. ¿El centro de datos posee UPS?

☒ SI ☐ NO

☐ Otra (por favor, especifique)

4. ¿El Generador está correctamente dimensionado de acuerdo a las capacidades de las UPS instaladas?

☒ SI ☐ NO

☐ Otra (por favor, especifique)

5. Supresión de Fuego: ¿Existe sistema de rociadores proactivo? (cuando se requieran)

☒ SI ☐ NO

Propuesta para la certificación TIER II del Centro de Datos de la Dirección General de Ingresos.

☐ Otra (por favor, especifique) _____

6. ¿El centro de datos posee piso elevado?

☒ SI ☐ NO

☐ Otra (por favor, especifique) _____

7. ¿El centro de datos cuenta con Lobby de entrada?

☒ SI ☐ NO

☐ Otra (por favor, especifique) _____

8. ¿Posee Control acceso de seguridad y monitoreo en puertas de salas de computadores con detección de intrusos?

☒ SI ☐ NO

☐ Otra (por favor, especifique) _____

9. ¿Existe Control de Humedad para sala de computadores a través de Humidificación?

☒ SI ☐ NO

☐ Otra (por favor, especifique) _____

10. ¿Existen PDUS de alimentación en todos los equipos de telecomunicaciones y computadores?

☒ SI ☐ NO

☐ Otra (por favor, especifique) _____

Anexo B: Cuadro comparativo Norma TIA 942 con Centro de Datos DGI.

Criterio	*Especificaciones Certificación Tier ll*	*Centro de Datos Dirección General de Ingresos*
Evaluación del Sitio	**El centro de datos debe de estar alejado de las siguientes instalaciones: Aeropuertos, Bases militares, Planta de productos químicos y fertilizantes.**	**El centro Nacional de Datos Fiscales tiene en sus alrededores un predio baldío así como las instalaciones colindan con la carretera. Se encuentra ubicado a 13 km de distancia de Aeropuertos, Bases militares, Planta de productos químicos y fertilizantes**
Evaluación del Sitio	**El centro de datos debe de estar fuera de Actividad sísmica, riesgo de inundaciones y fuego incontrolado.**	**El centro Nacional de Datos Fiscales de la DGI se encuentra en una zona fuera de actividad volcánica e inundaciones. Sin embargo colinda un con predio baldío, lo que podría provocar un incendio incontrolado y propagarse rápidamente al centro de datos.**
Evaluación Arquitectónica	**Estacionamiento separado para visitantes y empleados**	**La dirección general de ingresos cuenta con un estacionamiento separado para visitantes y empleados.**
Evaluación Arquitectónica	**Muros divisorios interiores para salas que no son para computadora**	**El centro de datos cuenta con muros que dividen las salas de monitoreo, sala donde se albergan los servidores, sala de telecomunicaciones y sala donde se encuentra la planta eléctrica.**
Evaluación Arquitectónica	**Debe de contar con pisos Falsos.**	**El centro de datos cuenta con Pisos elevados removibles. Sin embargo requiere manteniendo en algunos ladrillos.**
Evaluación del Sistema Eléctrico	**Ups, baterías Y sistema de enfriamiento.**	**El centro de datos cuenta con dos ups marca LADE y con un generador de energía de respaldo EATON, encargada de suministrar energía eléctrica a los equipos en caso de fallo de la energía comercial. Cuenta con dos unidades de precisión marca SCHNAIDER para el aclimatamiento del lugar.**
Evaluación de la Protección contra incendios	**Contar con un sistema de detección de incendios: Detectores de humos, calor o flama.**	**El centro d datos De la dirección general de ingresos cuenta con detectores de incendios de alerta temprana así como rociadores para suprimir el fuego.**

Criterio	***Especificaciones Certificación Tier ll***	***Centro de Datos Dirección General de Ingresos***
Evaluación de la Protección contra incendios	**En cuanto a medios manuales se debe de contar con bocas de incendios equipadas, extintores portátiles preferiblemente por gas en la sala (Dióxido de carbono).**	**El centro de datos cuenta con un extintor de incendio en cada sala del edificio.**
Evaluación de la Seguridad	**Sistemas biométricos: Llaves, Tarjetas, huella digital o retina.**	**Cada entrada al centro de datos cuenta con un sistema biométrico con huella digital, permitiendo el acceso solamente exclusivo a los administradores.**
Evaluación de la Seguridad	**Seguridad perimetral.**	**El centro de datos cuenta con seguridad perimetral sin embargo se puede ingresar a las afueras de las instalaciones.**
Evaluación de la Infraestructura, vías y espacios de cableado de telecomunicaciones	**Gabinetes y bastidores de telecomunicaciones y computadoras**	**Cuenta con Gabinetes y bastidores, algunos requieren de mantenimiento.**
Evaluación de la Infraestructura, vías y espacios de cableado de telecomunicaciones	**Cables etiquetados.**	**Los cables del centro de datos esta etiquetaos en la parte trasera pero no están etiquetados en la parte frontal.**

Anexo C: Nota Aclaratoria

Gobierno de Reconciliación y Unidad Nacional
El Pueblo, Presidente!

2018
UNID@S EN VICTORIAS! Por Gracia de Dios!

Managua 22 de octubre de 2018

A QUIEN CONCIERNE:

Por medio de la presente y a solicitud de la interesada, el ingeniero Roger David Deshon Meza, Subdirector de la División de Informática de la dirección General de Ingresos Certifica que

La compañera Josseline Jazmin Gomez Urbina desarrolló para la institución la propuesta denominada "**Propuesta para la certificación TIER II del Centro de Datos de la Dirección General de Ingresos"** cuya tutoría fue asignada a la MSc. Ing. Lizette Carolina Duarte Mora docente de la Universidad Nacional de Ingeniería (UNI).

Debidos a los protocolos de seguridad en cuanto a no poner en peligro la integridad de la información de dicha institución, no podrá mostrar la infraestructura actual del centro de datos para el debido proceso de defensa monográfica permitiendo hacer referencia mediante prototipos y gráficos elaborado en el desarrollo de la propuesta.

Atentamente,

Ing. Roger David Deshon Meza
Subdirector de la División de Informática
Dirección General de Ingresos

FE, FAMILIA Y COMUNIDAD!

CRISTIANA, SOCIALISTA, SOLIDARIA!
DIRECCIÓN GENERAL DE INGRESOS
Costado Norte de Catedral Metropolitana - 2248-9999 www.dgi.gob.ni

Bibliografía

(DGI), D. g. (16 de Febrero de 2018). *www.dgi.gob.ni*. Obtenido de Direccion general de ingresos: www.dgi.gob.ni

(Rasmussen. (16 de Agosto de 2018). *Implementación de centros de datos con eficiencia energética, .*

BICSI. (03 de 05 de 2018).

BICSI. (27 de 02 de 2018). *BICSI, Inc*. Obtenido de www.bicsi.org

cartagena, A. l. (24 de 05 de 2018).

cisco. (2018). Managua.

Gaceta. (16 de febrero de 2018). Obtenido de http://sajurin.enriquebolanos.org/vega/docs/Inaugurar%20-%20DGI%20Centro%20Datos%20Tecnologico%20-%2027%20Nov%2006.pdf

García Enrich , G. (26 de 02 de 2018). *METACOM.* Obtenido de http://www.metacom.cl/dinamicos/descargas/estandar-tia-1445699953.pdf

IBM. (2018). Managua.

Institute, U. (19 de febrero de 2018). *Uptime Institute* . Obtenido de https://uptimeinstitute.com/TierCertification/certMaps.php

NFPA, E. (08 de septiembre de 2018). *Estándar para la protección contra incendios de las instalaciones de telecomunicaciones.*

Norma EIA/TIA 568A . (2018). Managua.

Norma EIA/TIA 568A . (2018). Managua.

Norma NFPA 76. (2018). Managua.

normas aplicadas pragon. (2018). Managua.

odbc, b. (19 de Febrero de 2018). *Bloc.odbc.* Obtenido de http://blog.aodbc.es/2012/07/10/clasificacion-tier-en-el-datacenter-el-estandar-ansitia-942/

schneider-electric. (20 de agosto de 2018).

TI, A. (24 de 04 de 2018). *Data center de alta disponibilidad*.

TIA-607. (21 de Agosto de 2018).

TIA-942, V. g. (26 de 02 de 2018). *Vison general estandar TIA-942.*